Instant Wireless® Series

Wireless-G Broadband Router



Use this guide to install:

WRT54G

User Guide

LINKSYS®

COPYRIGHT & TRADEMARKS

LIMITED WARRANTY

Linksys guarantees that every Instant Wireless Wireless-G Broadband Router will be free from physical defects in material and workmanship for one year from the date of purchase, when used within the limits set forth in the Specifications section of this User Guide.

If the product proves defective during this warranty period, go to the Linksys website at *www.linksys.com* for complete RMA (Return Merchandise Authorization) assistance. You can also call Linksys Technical Support in order to obtain a RMA Number. BE SURE TO HAVE YOUR PROOF OF PURCHASE AND A BARCODE FROM THE PRODUCT'S PACKAGING ON HAND WHEN CALLING. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. When returning a product, mark the RMA Number clearly on the outside of the package and include a copy of your original proof of purchase. All customers located outside of the United States of America and Canada shall be held responsible for shipping and handling charges.

IN NO EVENT SHALL LINKSYS'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS OFFERS NO REFUNDS FOR ITS PRODUCTS. Linksys makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Linksys reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to:

Linksys P.O. Box 18558, Irvine, CA 92623.

SAFETY AND REGULATORY NOTICES

FCC STATEMENT

The Instant Wireless® Wireless-G Broadband Router has been tested and found to comply with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution: Any change or modification to the product not expressly approved by Linksys could void the user's authority to operate the device.

FCC RF Radiation Exposure Statement

To comply with the FCC and ANSI C95.1 RF exposure limits, the antenna(s) for this device must comply with the following:

- Access points with 2.4 GHz integrated antenna must operate with a separation distance of at least 20 cm from all persons using the cable provided and must not be co-located or operating in conjunction with any other antenna or transmitter.

End-users must be provided with specific operations for satisfying RF exposure compliance.

Note: Dual antennas used for diversity operation are not considered co-located.

Canadian Department of Communications Industry Canada (IC) Notice

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 et CNR-210 du Canada.

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."

" Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé à l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence. "

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys Group declares that the Instant Wireless® Series products included in the Instant Wireless® Series conform to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC, EMC directive 89/336/EEC, and Low Voltage directive 73/23/EEC:

For 11Mbps, 2.4 GHz access points with 100 mW radios, the following standards were applied:

- EMC: EN 301 489-1, EN 301.89-17
- Safety: EN 60950
- Radio: ETS 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC and/or the CEPT recommendation Rec 70.03.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

- Linksys Group vakuuttaa täten Instant Wireless® Wireless-G Broadband Router tyyppinen laite on direktiivin 1999/5/EY, direktiivin 89/336/EEC ja direktiivin 73/23/EEC oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.
- Linksys Group déclare que la Instant Wireless® Wireless-G Broadband Router est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC, la directive 89/336/EEC, et à la directive 73/23/EEC.
- Belgique B L'utilisation en extérieur est autorisé sur le canal 11 (2462 MHz), 12 (2467 MHz), et 13 (2472 MHz). Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.
- France F:
  2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le départment. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.
  Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.
  2.4 GHz Band: only channels 10, 11, 12, 13 (2457, 2462, 2467, and 2472 MHz respectively) may be used freely in France for indoor use. License required for outdoor installations.
  Please contact ART (http://www.art-telecom.fr) for procedure to follow.
- Deutschland D: Anmeldung im Outdoor-Bereich notwending, aber nicht genehmigungspflichtig. Bitte mit Händler die Vorgehensweise abstimmen.
- Germany D: License required for outdoor installations. Check with reseller for procedure to follow.
- Italia I: E' necessaria la concessione ministeriale anche per l'uso interno. Verificare con i rivenditori la procedura da seguire. L'uso per installazione in esterni non e' permessa.
- Italy I: License required for indoor use. Use with outdoor installations not allowed.
- The Netherlands NL License required for outdoor installations. Check with reseller for procedure to follow.
- Nederlands NL Licentie verplicht voor gebruik met buitenantennes. Neem contact op met verkoper voor juiste procedure.

UG-WRT54G-122402A JL

Table of Contents

Chapter 1: Introduction

The Wireless-G Broadband Router

Wireless-G is the upcoming 54Mbps wireless networking standard that’s almost five times faster than the widely deployed Wireless-B (802.11b) products found in homes, businesses, and public wireless hotspots around the country—but since they share the same 2.4GHz radio band, Wireless-G devices can also interoperate with existing 11Mbps Wireless-B equipment.

Since both standards are built in, you can protect your investment in existing 802.11b infrastructure, and migrate to the new screaming fast Wireless-G standard as your needs grow.

The Linksys Wireless-G Broadband Router is really three devices in one box. First, there’s the Wireless Access Point, which lets you connect Wireless-G or Wireless-B devices to the network. There’s also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices. Connect four PCs directly, or daisy-chain out to more hubs and switches to create as big a network as you need. Finally, the Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

To protect your data and privacy, the Wireless-G Broadband Router can encrypt all wireless transmissions. The Router can serve as a DHCP Server, has NAT technology to protect against Internet intruders, supports VPN pass-through, and can be configured to filter internal users’ access to the Internet. Configuration is a snap with the web browser-based configuration utility.

With the Linksys Wireless-G Broadband Router at the center of your home or office network, you can share a high-speed Internet connection, files, printers, and multi-player games with the flexibility, speed, and security you need!

Features

- Compatibility with Draft 802.11g (2.4GHz) and 802.11b (2.4GHz) Standards
- Setup Wizard for Easy Installation
- Wireless Security with up to 128-bit WEP Encryption
- Enhanced Security Management Functions: Internet Access Policies with Time Schedules, Website Blocking, IP and MAC Address Filtering; Port Filtering; Wireless MAC Address Filtering; and NAT Technology
- Access Your Corporate Network Remotely through Virtual Private Networking (VPN)—Supports IPSec and PPTP Pass-Through
- Supports Dynamic Domain Name System (DDNS) Service, Static and Dynamic Routing (RIP1 and 2), DMZ Hosting
- Web-based Utility for Easy Configuration from Any Web Browser
- DHCP Server Capability to Assign IP Addresses Automatically
- All Ethernet Ports Support Auto-Crossover (MDI/MDI-X)—No Need for Crossover Cables
- Free Technical Support—24 Hours a Day, 7 Days a Week, Toll-Free US Calls
- 1-Year Limited Warranty

The Router's Functions

Simply put, a router is a network device that connects two networks together.

In this instance, the Router connects your Local Area Network (LAN), or the group of PCs in your home or office, to the Internet. The Router processes and regulates the data that travels between these two networks.

The Router's NAT feature protects your network of PCs so users on the public, Internet side cannot "see" your PCs. This is how your network remains private. The Router protects your network by inspecting every packet coming in through the Internet port before delivery to the appropriate PC on your network. The Router inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate PC on the LAN side.

Remember that the Router's ports connect to two sides. The LAN ports connect to the LAN, and the Internet port connects to the Internet. The LAN and Internet ports transmit data at 10/100Mbps.

IP Addresses

What's an IP Address?

IP stands for Internet Protocol. Every device on an IP-based network, including PCs, print servers, and routers, requires an IP address to identify its "location," or address, on the network. This applies to both the Internet and LAN connections. There are two ways of assigning an IP address to your network devices. You can assign static IP addresses or use the Router to assign IP addresses dynamically.

Note: Since the Router is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address."

Since the Router uses NAT technology, the only IP address that can be seen from the Internet for your network is the Router's Internet IP address.

However, even this Internet IP address can be blocked, so that the Router and network seem invisible to the Internet—see the Block WAN Requests description under Filters in "Chapter 6: The Router's Web-based Utility."

Static IP Addresses

A static IP address is a fixed IP address that you assign manually to a PC or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses must be unique and are commonly used with network devices such as server PCs or print servers.

If you use the Router to share your cable or DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Router. You can get that information from your ISP.

Dynamic IP Addresses

A dynamic IP address is automatically assigned to a device on the network, such as PCs and print servers. These IP addresses are called "dynamic" because they are only *temporarily* assigned to the PC or device. After a certain time period, they expire and may change. If a PC logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will automatically assign it a new dynamic IP address.

DHCP (Dynamic Host Configuration Protocol) Servers

PCs and other network devices using dynamic IP addressing are assigned a new IP address by a DHCP server. The PC or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

A DHCP server can either be a designated PC on the network or another network device, such as the Router. By default, the Router's DHCP Server function is enabled.

If you already have a DHCP server running on your network, you *must* disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Router, see the DHCP section in "Chapter 6: The Router's Web-based Utility."

Router Setup Overview

Note: You should always run the Setup CD-ROM to configure the Router for Internet access. If you wish to manually configure the Router, you may follow the instructions in the Quick Installation guide or this User Guide.

This User Guide covers the steps for setting up a network with the Router (see Figure 1-1). After going through "Chapter 2: Getting to Know the Wireless-G Broadband Router," most users will only need to use the following chapters:

- Chapter 3: Connect the Router
  This chapter instructs you on how to connect a cable or DSL modem to the Router and connect your PC(s) to the Router.

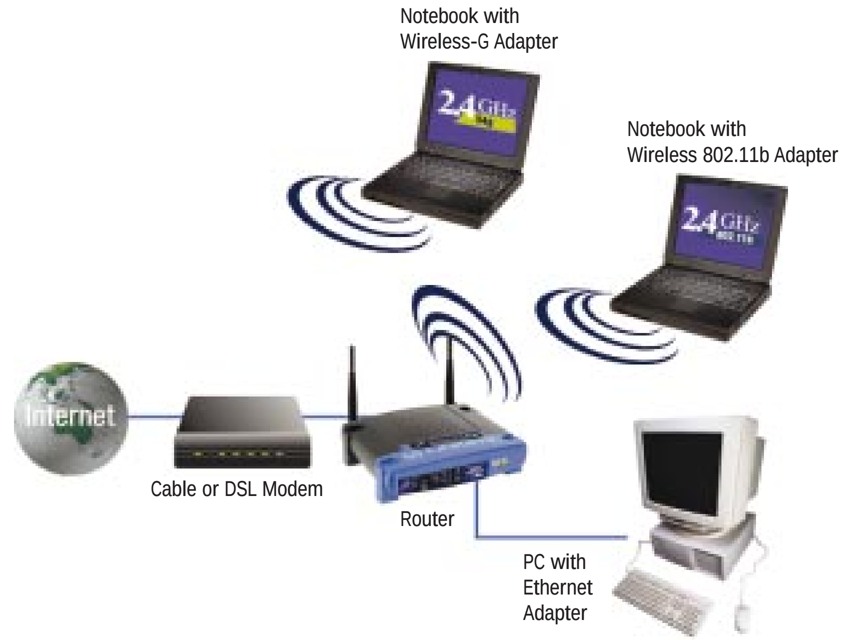


Figure 1-1

- Chapter 4: Configure the PCs
  This chapter instructs you on how to configure your PCs to be DHCP clients, if you have previously set static IP addresses on your PCs.

- Chapter 5: Configure the Router's Basic Settings
  This chapter explains how to configure the Router using your web browser and the Router's web-based utility. You will configure the Router for Internet access using the settings provided by your ISP.

When you're finished with these basic steps, you will be ready to connect to the Internet. You can also modify the Router's settings further; for example, you can adjust security features and other settings to enable online gaming (see "Chapter 6: The Router's Web-based Utility").

Chapter 2: Getting to Know the Wireless-G Broadband Router

The Router's Back Panel



Figure 2-1

The Router's ports are located on the Router's back panel.

Internet The Internet port is where you connect your cable or DSL modem through an Ethernet network cable. Your modem connection will not work from any other port.

Ports 1-4 These four LAN (Local Area Network) ports connect to network devices, such as PCs, print servers, and network attached storage (NAS). Each of the ports will auto-detect whether a straight-through or crossover cable is plugged into it, so there is no need for an uplink port. Any one of the four ports can serve as an uplink port to other network devices.

Power The Power port is where you will connect the power adapter.

The Reset Button

The **Reset** button can be used in one of two ways:

1. Reboot the Router while keeping all of its settings.

   If the Router is having problems connecting to the Internet, press the **Reset** button for just a moment with a paper clip or a pencil tip. This clears up any jammed connections, and is similar to pressing the **Reset** button on your PC to reboot it.

2. Restore the Router's factory defaults and clear all of its settings, including a new password or wireless settings.

   If you are experiencing extreme problems with the Router and have tried all other troubleshooting measures, press the **Reset** Button and hold it down for 10 seconds.

The Router's Front Panel LEDs



Figure 2-2

The Router's LEDs display information about the Router's status.

Power *Green*. This LED lights up when the Router is powered on.

DMZ *Green*. The **DMZ** LED lights up when the DMZ hosting feature is being used.

Diag *Red*. The **Diag** LED lights up when the Router goes through its self-diagnosis mode during every boot-up. It will turn off upon successful completion of the diagnosis.

If this LED stays on for one minute or longer, see "Appendix A: Troubleshooting."

The WLAN Indicators

Act *Green*. When the **Act** LED flickers, the wireless network is active.

Link *Green*. When the **Link** LED is continuously lit, the wireless network is available.

The LAN Indicators

Link/Act *Green*. The **Link/Act** LED serves two purposes. If the LED is continuously lit, the Router is successfully connected to a device through the corresponding port. If the LED is flickering, the Router is actively sending or receiving data over that port.

Full/Col *Green*. The **Full/Col** LED also serves two purposes. If this LED is lit up solidly, the connection made through the corresponding port is running in full duplex mode. If the LED flickers, the connection is experiencing collisions (when two PCs send data at the same time). Infrequent collisions are normal.

100 *Orange*. The **100** LED lights up when a successful 100Mbps connection is made through the corresponding port.

If this LED does not light up, then your connection speed is 10Mbps.

The Internet Indicators

Link/Act *Green*. The **Link/Act** LED lights up when a successful connection is made between the Router and your cable or DSL modem (the Internet). The **Link/Act** LED flickers when the Router is sending or receiving data over the **Internet** port.

Full/Col *Green*. The **Full/Col** LED serves two purposes. If this LED is lit up solidly, the connection made through the corresponding port is running in full duplex mode. If the LED flickers, the connection is experiencing collisions (when two PCs send data at the same time). Infrequent collisions are normal.

100 *Orange*. The **100** LED lights up when a successful 100Mbps connection is made through the corresponding port.

If this LED does not light up, then your connection speed is 10Mbps.

Proceed to "Chapter 3: Connect the Router."

Chapter 3: Connect the Router

Overview

The Router's setup consists of more than simply plugging hardware together. You will have to configure your networked PCs to accept the IP addresses that the Router assigns them (if applicable), and you will also have to configure the Router with setting(s) provided by your Internet Service Provider (ISP).

The installation technician from your ISP should have left the setup information for your modem with you after installing your broadband connection. If not, you can call your ISP to request that data.

Once you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Router.

If you want to use a PC with an Ethernet adapter to configure the Router, go to "Wired Connection to a PC." If you want to use a PC with a wireless adapter to configure the Router, go to "Wireless Connection to a PC and Boot-Up."

Wired Connection to a PC

1. Before you begin, make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.

2. Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the Router, and the other end to an Ethernet port on a PC.



Figure 3-1

   Repeat this step to connect more PCs, a switch, or other network devices to the Router.

3. Connect a different Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel. This is the only port that will work for your modem connection.



Figure 3-2

4. Power on the cable or DSL modem.

5. Connect the power adapter to the Router's Power port, and then plug the power adapter into a power outlet.

Note: You should always plug the Router's power adapter into a power strip with surge protection.



Figure 3-3

- The **Power** LED on the front panel will light up green as soon as the power adapter is connected properly.

- The **Diag** LED will light up red for a few seconds. It will turn off when the self-test is complete. If this LED stays on for one minute or longer, see "Appendix A: Troubleshooting."

6. Power on one of your PCs.

Have you checked that the **Link/Act** LEDs for all your LAN connections and the **Link** LED for your Internet connection light up?

If all of your **Link** LEDs are not lighting up, make sure that all your cables are securely plugged in, and that all of your hardware is powered on properly. Verify that the modem is plugged into the Internet port on the Router.

Wireless Connection to a PC

If you want to use a wireless connection to access the Router, follow these instructions:

1. Before you begin, make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.

2. Connect an Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel. This is the only port that will work for your modem connection.



Figure 3-4

3. Power on the cable or DSL modem.

4. Connect the power adapter to the Power port, and then plug the power adapter into a power outlet.

Note: You should always plug the Router's power adapter into a power strip with surge protection.

- The **Power** LED on the front panel will light up green as soon as the power adapter is connected properly.

- The **Diag** LED will light up red for a few seconds and turn off when the self-test is complete. If this LED stays on for one minute or longer, see "Appendix A: Troubleshooting."

4. Power on one of the PCs on your wireless network(s).

5. For initial access to the Router through a wireless connection, make sure the PC's wireless adapter has its SSID set to **linksys** (the Router's default setting), and its WEP encryption is **disabled**. After you have accessed the Router, you can change the Router and this PC's adapter settings to match the your usual network settings.

Note: You should always change the SSID from its default, **linksys**, and enable WEP encryption.

The Router's hardware installation is now complete.
Go to "Chapter 4: Configure the PCs."

Chapter 4: Configure the PCs

Overview

The instructions in this chapter will help you configure each of your computers to be able to communicate with the Router.

To do this, you need to configure your PC's network settings to obtain an IP (or TCP/IP) address automatically, so your PC can function as a DHCP client. Computers use IP addresses to communicate with the Router and each other across a network, such as the Internet.

First, find out which Windows operating system your computer is running. You can find out by clicking the **Start** button. Read the side panel of the Start menu to find out which operating system your PC is running.

You may need to do this for each computer you are connecting to the Router.

The next few pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using. Make sure that an Ethernet or wireless adapter (also known as a network adapter) has been successfully installed in each PC you will configure. Once you've configured your computers, continue to "Chapter 5: Configure the Router's Basic Settings."

Important: By default Windows 98, 2000, Me, and XP has TCP/IP installed and set to obtain an IP address automatically.

If your PC does not have TCP/IP installed, click **Start** and then **Help**. Search for the keyword **TCP/IP**. Then follow the instructions to install TCP/IP.

Configuring Windows 98 and Millennium PCs

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Double-click the **Network** icon.

2. On the Configuration tab, select the **TCP/IP** line for the applicable Ethernet adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. If the word **TCP/IP** appears by itself, select that line. Click the **Properties** button.

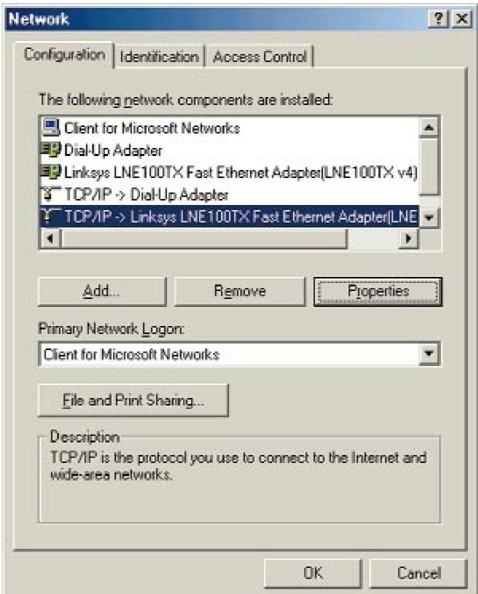


Figure 4-1

3. Click the **IP Address** tab. Select **Obtain an IP address automatically**.

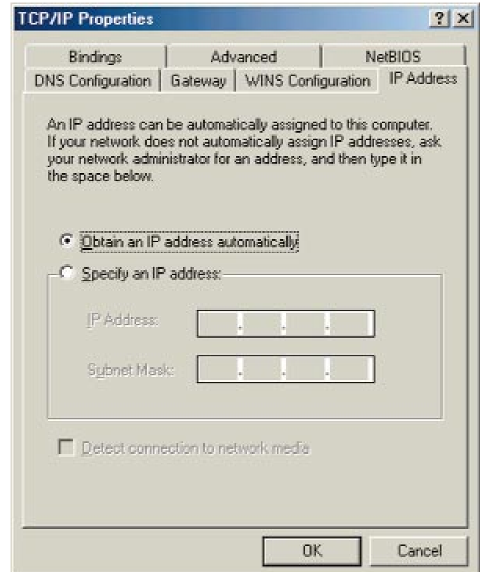


Figure 4-2

4. Now click the **Gateway** tab, and verify that the *Installed Gateway* field is blank. Click the **OK** button.

5. Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, e.g., D:\win98, D:\win9x, etc. (if “D” is the letter of your CD-ROM drive).

6. Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

Go to “Chapter 5: Configure the Router’s Basic Settings.”

Configuring Windows 2000 PCs

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Double-click the **Network and Dial-up Connections** icon.

2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button.

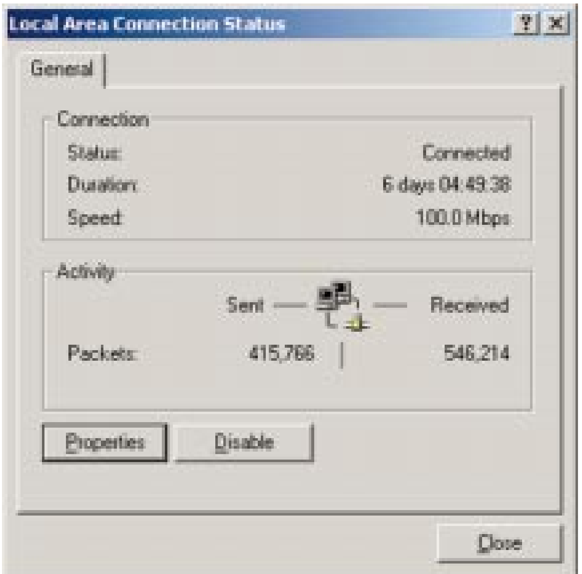


Figure 4-3

3. Make sure the box next to *Internet Protocol (TCP/IP)* is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.



Figure 4-4

4. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.



Figure 4-5

5. Restart your computer.

Go to "Chapter 5: Configure the Router's Basic Settings."

Configuring Windows XP PCs

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click the **Start** button and then the **Control Panel** icon. Click the **Network and Internet Connections** icon. Then click the **Network Connections** icon.

2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button.



Figure 4-6

3. Make sure the box next to *Internet Protocol (TCP/IP)* is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.

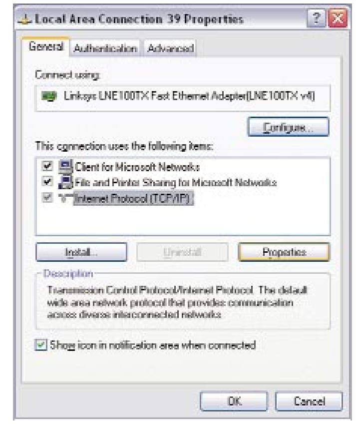


Figure 4-7

4. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.



Figure 4-8

Go to “Chapter 5: Configure the Router’s Basic Settings.”

Chapter 5: Configure the Router's Basic Settings

This chapter will show you how to configure the Router to function in your network and gain access to the Internet through your Internet Service Provider (ISP). Detailed description of the Router's web-based utility can be found in "Chapter 6: The Router's Web-based Utility."

The instructions from your ISP tell you how to set up your PC for Internet access. Because you are now using the Router to share Internet access among several computers, you will use the setup information to configure the Router instead of your PC. You only need to configure the Router once using the first computer you set up.

1. Open your web browser. Enter **http://192.168.1.1** (the Router's default IP address) in the web browser's *Address* field. Press the **Enter** key.



Figure 5-1

2. An *Enter Network Password* window, shown in Figure 5-2, will appear. (Windows XP users will see a similar screen.) Leave the *User Name* field empty, and enter **admin** in lowercase letters in the *Password* field (**admin** is the default password). Then, click the **OK** button.



Figure 5-2

Note: For added security, you should change the password through the *Security* screen of the web-based utility.

3. The web-based utility will appear with the *Setup* tab selected. Select the time zone for your location. If your location experiences daylight savings, leave the checkmark in the box next to *Automatically adjust clock for daylight saving changes*.

4. Based on the setup instructions from your ISP, you may need to provide the Host Name and Domain Name (usually cable ISPs require them). These fields allow you to provide a host name and domain name for the Router and are usually left blank.

   The values for the Router's LAN IP Address and Subnet Mask are shown on the *Setup* screen. The default values are 192.168.1.1 for the IP Address and 255.255.255.0 for the Subnet Mask.

5. The Router supports four connection types: Automatic Configuration - DHCP (obtain an IP automatically), Static IP, PPPoE, and PPTP. These types are listed in the drop-down menu for the Configuration Type setting. Each *Setup* screen and available features will differ depending on what kind of connection type you select. Proceed to the instructions for the connection type you are using, and then continue to step 6.

IMPORTANT: If you have previously enabled any **Internet-sharing proxy server software** on any of your PCs, you must disable it now.

Some examples of Internet-sharing software are Internet LanBridge, Wingate, ICS, and Sygate. To disable your Internet-sharing software:

- If you are running Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxies**. Click **Direct Connection to the Internet**.
- If you are running Internet Explorer 5.x or higher, click **Tools**, **Settings**, **Control Panel**, **Internet Options**, **Connections**, and **LAN Settings**. Remove checkmarks from all three boxes. Click the **OK** button to continue.

You must also disable any **Internet log-on software** (such as Ivasion Winpoet or Enternet 300) and any **firewall software** (such as ZoneAlarm and Watchdog) on all of your PCs.

Automatic Configuration - DHCP

If you are connecting through DHCP or a dynamic IP address from your ISP, perform these steps:

A. Keep the default setting, **Automatic Configuration - DHCP**, as the Configuration Type.

B. Click the **Apply** button to save the setting, or click the **Cancel** button to clear the setting and start over. When you are finished, proceed to step 6.

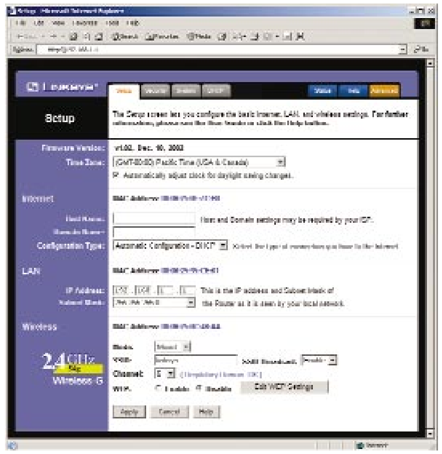


Figure 5-3

Static (or Fixed) IP Address

If you are connecting through a static or fixed IP address from your ISP, perform these steps:

A. Select **Static IP** as the Configuration Type.

B. Enter the **Internet IP Address**.

C. Enter the **Subnet Mask**.

D. Enter the **Default Gateway**.

E. Enter the **DNS** in the 1, 2, and/or 3 fields. You need to enter at least one DNS address.

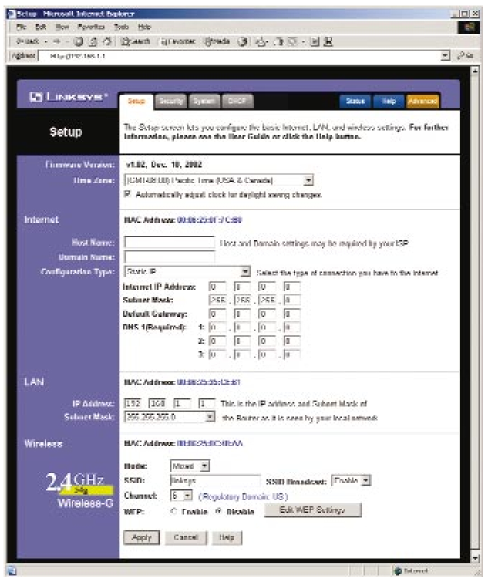


Figure 5-4

F. Click the **Apply** button to save the settings, or click the **Cancel** button to clear the settings and start over. When you are finished, proceed to step 6.

PPPoE

If your DSL provider says that you are connecting through PPPoE (you use a user name and password to access the Internet), perform these steps:

A. Select **PPPoE** as the Configuration Type.

B. Enter the **User Name**.

C. Enter the **Password**.

D. Click the **Apply** button to save the settings, or click the **Cancel** button to clear the settings and start over. When you are finished, proceed to step 6.

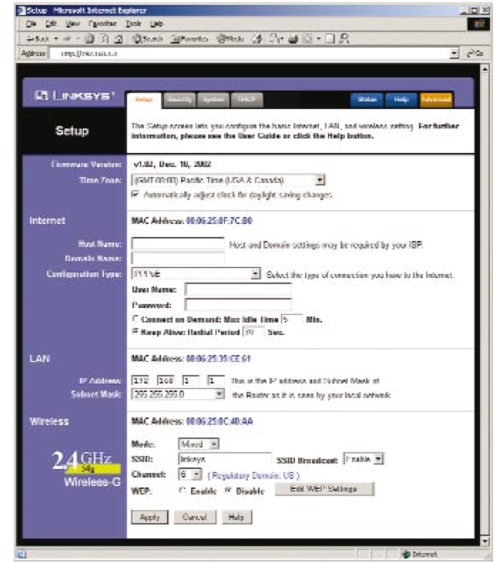


Figure 5-5

Important: If you enable PPPoE, remember to remove any PPPoE applications already installed on any of your PCs.

PPTP

PPTP is a service used in Europe only. If you are using a PPTP connection, check with your ISP for the necessary setup information.

After you have entered your setup information, click the **Apply** button to save the settings, or click the **Cancel** button to clear the settings and start over. When you are finished, proceed to step 6.



Figure 5-6

6. To configure the Router for your wireless network(s), perform these steps:

A. If you have Wireless-G and 802.11b devices in your network, then keep the default *Mode* setting, **Mixed**. If you have only Wireless-G devices, select **G-Only**. If you want to disable wireless networking, select **Disable**.

B. Customize the **SSID** and **Channel** settings as needed. For added security, you should change the default SSID (**linksys**) to a unique name. Then click the **Apply** button to save your changes. For more information, refer to "Chapter 6: The Router's Web-based Utility."

C. To enable WEP encryption (recommended), click the **Enable** radio button next to *WEP*. Then click the **Edit WEP Settings** button, and customize the WEP encryption settings as needed. Click the **Apply** button to save your settings. For more information, refer to "Chapter 6: The Router's Web-based Utility."

7. If you haven't already done so, click the **Apply** button to save your Setup settings. Close the web browser.

8. Restart your computers so that they can obtain the Router's new settings.

Test the setup by opening your web browser from any computer and entering *http://www.linksys.com/registration*.



Figure 5-7

If you need more details or advanced setting information, please refer to "Chapter 6: The Router's Web-based Utility" or the Linksys support website at *support.linksys.com*.

Congratulations! You've successfully configured the Router.

If you are unable to reach our website, you may want to review what you did in this section or refer to "Appendix A: Troubleshooting."

Proceed to "Chapter 6: The Router's Web-based Utility" for more details and advanced settings information.

Chapter 6: The Router's Web-based Utility

Overview

Use the Router's web-based utility to administer it. This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Router.

The *Setup*, *Security*, *System*, *DHCP*, *Status*, and *Help* screens are available for basic setup. For advanced setup, click the **Advanced** tab to access these screens: *Advanced Wireless*, *Filters*, *Port Forwarding*, *Routing*, and *DDNS*.

How to Access the Web-based Utility

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Then press **Enter**.



Figure 6-1

A password request page, shown in Figure 6-2 will pop up. (Windows XP users will see a similar screen.) Leave the *User Name* field blank, and enter **admin** (the default password) in the *Password* field. Then click the **OK** button.



Figure 6-2

Note: For added security, you should always change the password through the *Security* screen of the web-based utility.

To save your changes on any page, click the **Apply** button. To cancel any unsaved changes on any page, click the **Cancel** button. To get additional information about any screen's features, click the **Help** button.

Setup

The *Setup* screen is the first screen you see when you access the web-based utility. If you have already installed and set up the Router, you have already seen this screen and properly configured all of the screen's values.

Firmware Version This shows the version and date of the firmware you are using. Future versions of the Router's firmware will be posted and available for download on the Linksys website at *www.linksys.com*.

Time Zone Select the time zone for your location. If your location experiences daylight savings, leave the checkmark in the box next to *Automatically adjust clock for daylight saving changes*.

Internet

MAC Address The MAC Address of the Internet interface is displayed here.

Host Name and **Domain Name** These fields allow you to supply a host and domain name for the Router. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

Configuration Type The Router supports four connection types: Automatic Configuration - DHCP, Static IP, PPPoE, and PPTP. Each *Setup* screen and available features will differ depending on what kind of connection type you select.

Note: You can verify that the Internet configuration settings are correct by successfully connecting to the Internet.

Automatic Configuration - DHCP

By default, the Router's Configuration Type is set to Automatic Configuration - DHCP, and it should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

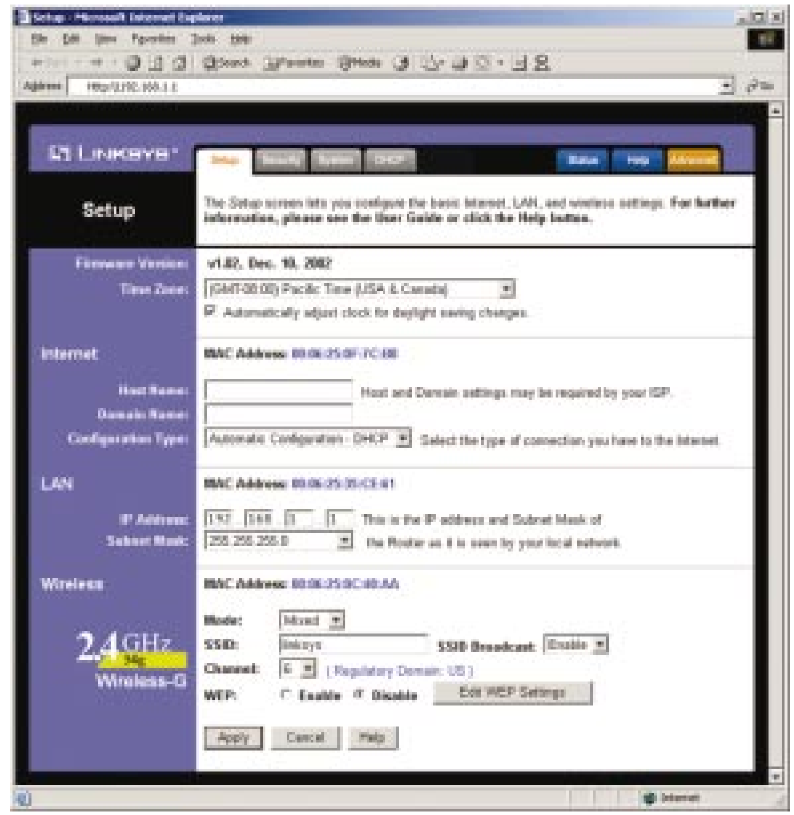


Figure 6-3

Static IP

If you are required to use a permanent IP address to connect to the Internet, then select **Static IP**.

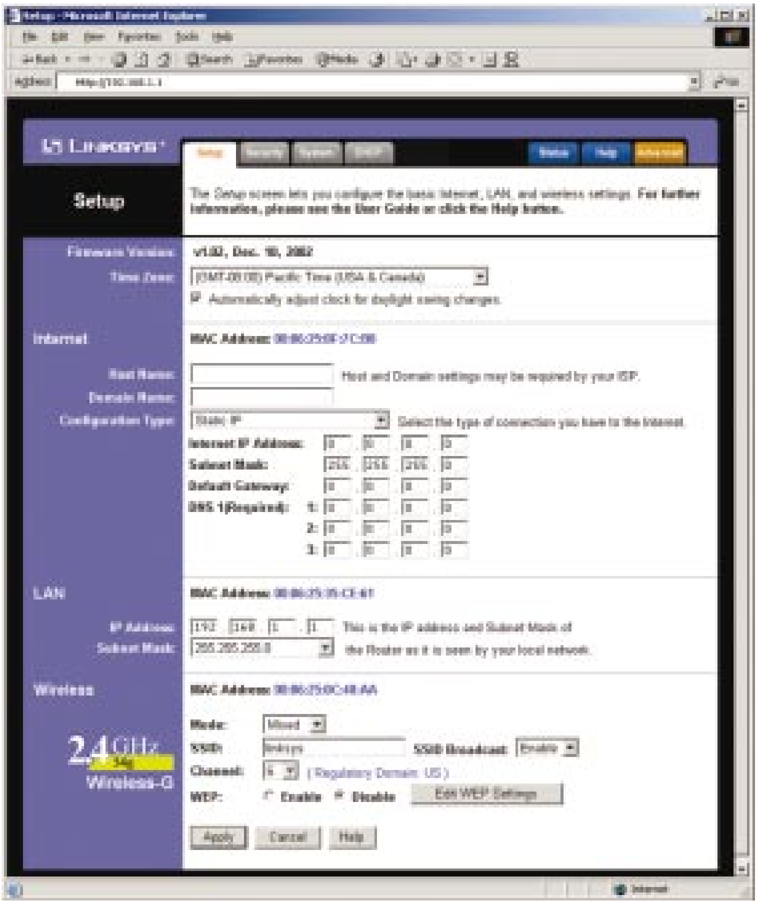


Figure 6-4

Internet IP Address This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address.

DNS 1 (Required) and DNS 2-3 (Optional) Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.

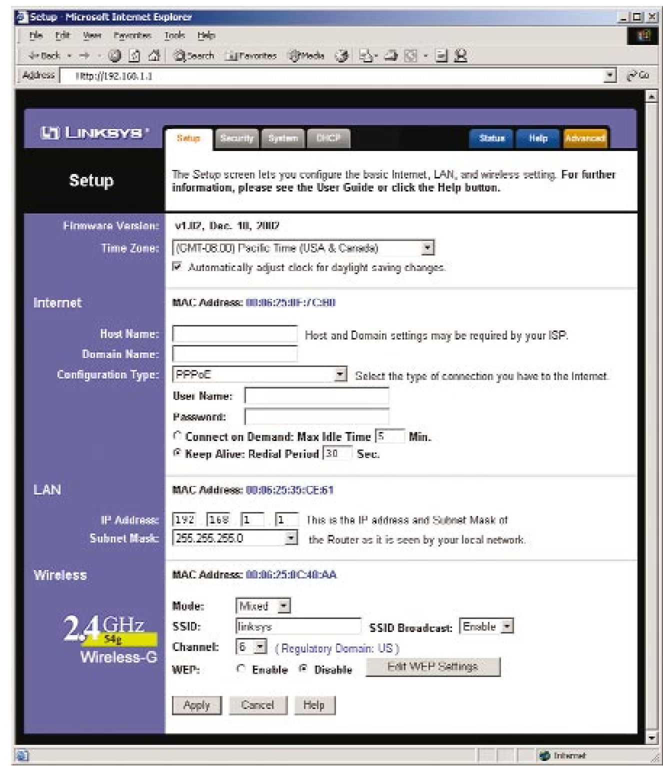


Figure 6-5

User Name and Password Enter the **User Name** and **Password** provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Keep Alive Option: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only (see Figure 6-8).

Internet IP Address This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the Default Gateway Address.

User Name and Password Enter the **User Name** and **Password** provided by your ISP.

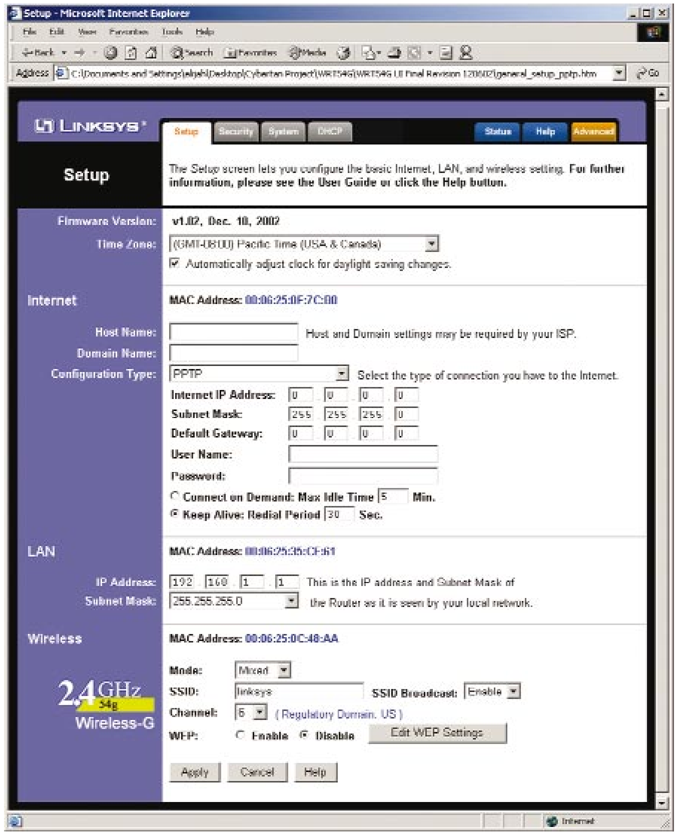


Figure 6-6

Important: For ADSL users, if you enable PPPoE, remember to remove any PPPoE applications that are already installed on any of your PCs.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Keep Alive Option: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. To use this option, click the radio button next to **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

LAN

MAC Address The MAC Address of the LAN interface is displayed here.

IP Address and LAN Subnet Mask The values for the Router's IP Address and Subnet Mask are shown here. The default values are 192.168.1.1 for the IP Address and 255.255.255.0 for the Subnet Mask.

Wireless 2.4GHz, 54g, Wireless-G

MAC Address The MAC Address of the wireless interface is displayed here.

Mode If you have Wireless-G and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only Wireless-G devices, select **G-Only**. If you want to disable wireless networking, select **Disable**.

SSID The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all devices in your wireless network. For added security, Linksys recommends that you change the default SSID (**linksys**) to a unique name of your choice.

SSID Broadcast When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enable**. If you do not want to broadcast the Router's SSID, then select **Disable**.

Channel Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All devices in your wireless network must use the same channel in order to function correctly.

WEP An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode data transmissions, all devices-Wireless-G and 802.11b-in a network must use an identical WEP key. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

To enable WEP encryption, click the **Enable** radio button. Then click the **Edit WEP Settings** button to configure the WEP settings. To disable WEP encryption, keep the default setting, **Disable**.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

2.4GHz, 54g, Wireless-G (WEP)

The *2.4GHz, 54g, Wireless-G (WEP)* screen allows you to configure your WEP settings. WEP encryption should always be enabled to increase the security of your wireless network.

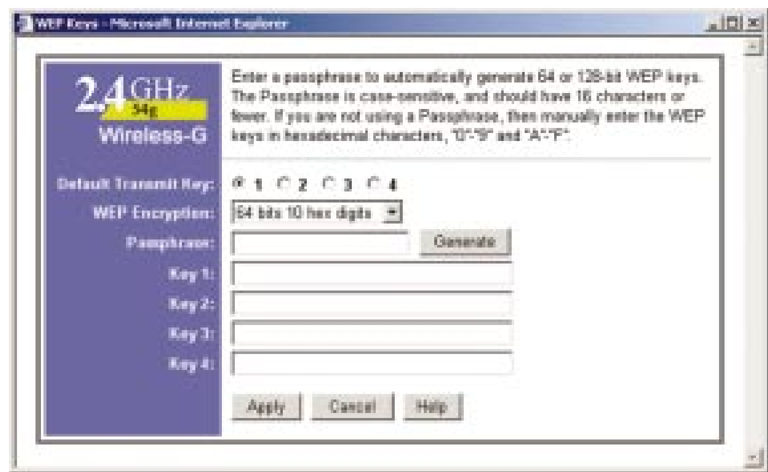


Figure 6-7

Default Transmit Key Select which WEP key (1-4) will be used when the Router sends data. Make sure the receiving device is using the same key.

WEP Encryption Select the level of WEP encryption you wish to use, **64-bit 10 hex digits** or **128-bit 26 hex digits**. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

Passphrase Instead of manually entering WEP keys, you can enter a Passphrase. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, enter the WEP key manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

Keys 1-4 WEP keys enable you to create an encryption scheme for wireless LAN transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.)

If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F".

Note: All Wireless-G and 802.11b devices in your network must use the same Passphrase or WEP key.

Check all the values, and click the **Apply** button to save your WEP settings. To cancel any changes you've entered on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Security

The *Security* screen allows you to change the Router's security settings. You should change the factory default password, which is **admin**, to your own as soon as possible. All users who try to access the Router's web-based utility or Setup Wizard will be prompted for the Router's password.

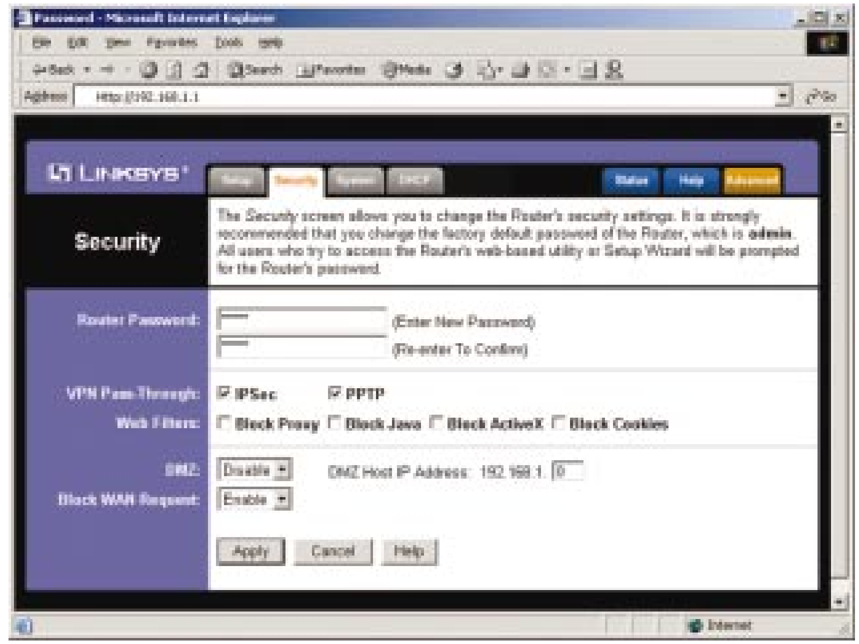


Figure 6-8

Router Password The new Password must not exceed 32 characters in length and must not include any spaces. Enter the new Password in the second field to confirm it.

VPN Pass-Through Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the Router supports IPSec Pass-Through and PPTP Pass-Through.

> ***IPSec*** - Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, IPSec Pass-Through is enabled by default. To disable IPSec Pass-Through, uncheck the box next to *IPSec*.

PPTP - Point-to-Point Tunneling Protocol is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP tunnels to pass through the Router, PPTP Pass-Through is enabled by default. To disable PPTP Pass-Through, uncheck the box next to *PPTP*.

Web Filters Using the Web Filters feature, you may enable up to four specific filtering methods.

Block Proxy - Use of WAN proxy servers may compromise the Router's security. Denying Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the **Block Proxy** box.

Block Java - Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. To enable Java filtering, click the **Block Java** box.

Block ActiveX - ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click the **Block ActiveX** box.

Block Cookies - A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click the **Block Cookies** box.

DMZ The DMZ hosting feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

1. To expose one PC, select **Enable**.
2. Enter the computer's IP address in the *DMZ Host IP Address* field.
3. Click the **Apply** button.

Block WAN Request By enabling the Block WAN Request feature, you can prevent your network from being "pinged," or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Select **Disable** to disable this feature.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

System

The *System* screen lets you control a variety of the Router's general features, from restoring factory defaults to enabling its remote management capability.

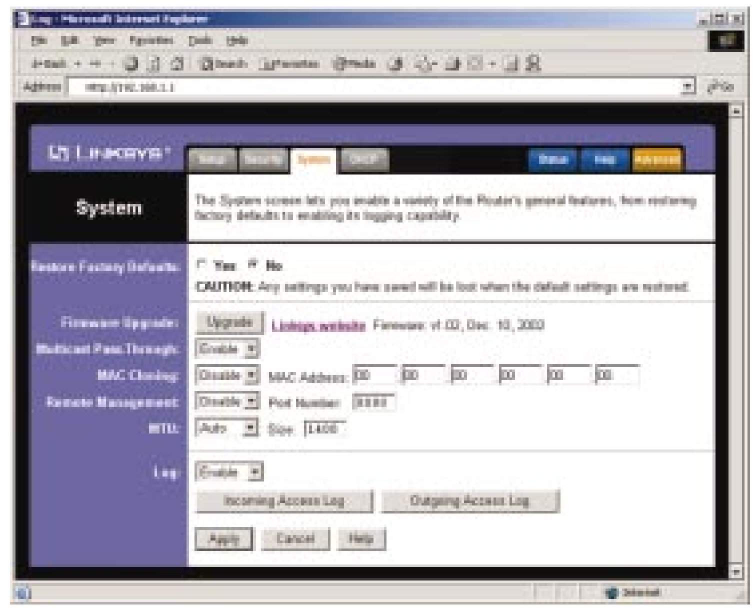


Figure 6-9

Restore Factory Defaults Click the **Yes** button to reset all configuration settings to their default values, and then click the **Apply** button. Any settings you have saved will be lost when the default settings are restored. This feature is disabled by default.

Upgrade Firmware New firmware versions are posted at *www.linksys.com* and can be downloaded for free. If the Router already works well, there's no need to download a newer firmware version, unless that version has a new feature that you want to use. (To learn about any new firmware with new features, visit *www.linksys.com*.)

> **Note:** By upgrading the Router's firmware, you may lose the Router's configuration settings, so make sure you write down the Router's settings before you upgrade its firmware.

To upgrade the Router's firmware:

1. Download the firmware upgrade file from *www.linksys.com*, and extract the file using a file archive utility such as WinZip.

2. Click the **Upgrade** button.

3. On the *Upgrade Firmware* screen (see Figure 6-10), click the Browse button to find the firmware upgrade file you extracted.



Figure 6-10

4. Double-click the firmware upgrade file you extracted.

5. Click the **Upgrade** button, and follow the on-screen instructions.

> **Important:** When you are upgrading the firmware, do NOT turn off the Router, and do NOT press the Reset button.

Multicast Pass-Through IP Multicasting occurs when a single data transmission is sent to multiple recipients at the same time. Using the Multicast Pass-Through feature, the Router allows IP multicast packets to be forwarded to the appropriate computers. Keep the default setting, **Enable**, to support the feature, or select **Disable** to disable it.

MAC Cloning You can clone the MAC address of your PC's network adapter onto the Router.

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require that you register the MAC address of your PC's network adapter, which was connected to your cable or DSL modem during installation. To avoid calling your ISP and changing the MAC address that is registered with the ISP, follow these instructions:

1. Select **Enable**.

2. Enter your adapter's MAC address in the *MAC Address* field.

3. To save your new settings, click the **Apply** button. To cancel your changes, click the **Cancel** button. To get more information about the features, click the **Help** button.

To disable MAC address cloning, keep the default setting, **Disable**.

If you do not know your adapter's MAC address, follow these instructions:

1. Click the **Start** button, and select **Run**.

2. Enter **command** in the field provided, and press the **OK** button.

3. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.

4. Write down your adapter's physical address; this is the adapter's MAC address.

Remote Management This feature allows you to manage your Router from a remote location, via the Internet. To disable this feature, keep the default setting, **Disable**. To enable this feature, select **Enable**, and use the specified port (default is **8080**) on your PC to remotely manage the Router. You must also change the Router's default password to one of your own, if you haven't already. A unique password will increase security.

To remotely manage the Router, enter **http://xxx.xxx.xxx.xxx:8080** (the x's represent the Router's Internet IP address, and 8080 represents the specified port) in your web browser's *Address* field. You will be asked for the Router's password. After successfully entering the password, you will be able to access the Router's web-based utility.

Note: If the Remote Management feature is enabled, anyone who knows the Router's Internet IP address and password will be able to alter the Router's settings.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, **Auto**, to have the Router select the best MTU for your Internet connection. To specify a MTU size, select **Manual**, and enter the value desired (default is **1400**). You should leave this value in the 1200 to 1500 range.

Log The Router can keep logs of all traffic for your Internet connection. To disable the Log function, keep the default setting, **Disable**. To monitor traffic between the network and the Internet, select **Enable**.

Temporary logs can be accessed by clicking either the **Incoming Access Log** or **Outgoing Access Log** button.

The Incoming Access Log gives you a log of all the incoming Internet traffic, displaying the Source IP address and Destination Port Number of the Router for each activity (see Figure 6-11). Click the **Refresh** button to update the logs. Click the **Close** button to return to the *System* screen.

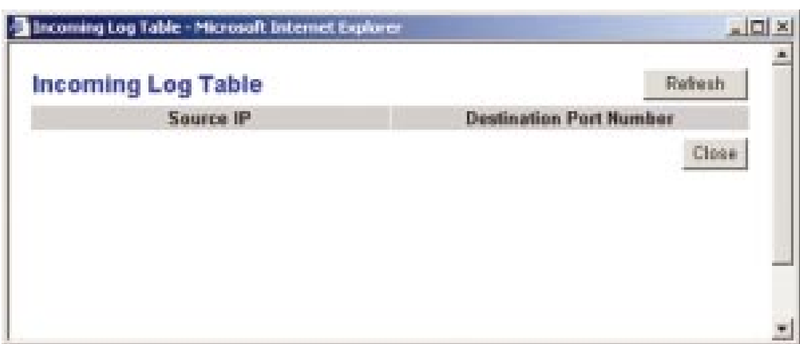


Figure 6-11

The Outgoing Access Log gives you a log of all outgoing Internet traffic. For each activity, it displays the LAN IP address, the Destination URL or IP address of the Internet site accessed, as well as the Service/Port Number used (see Figure 6-12). Click the **Refresh** button to update the logs. Click the **Close** button to return to the *System* screen.

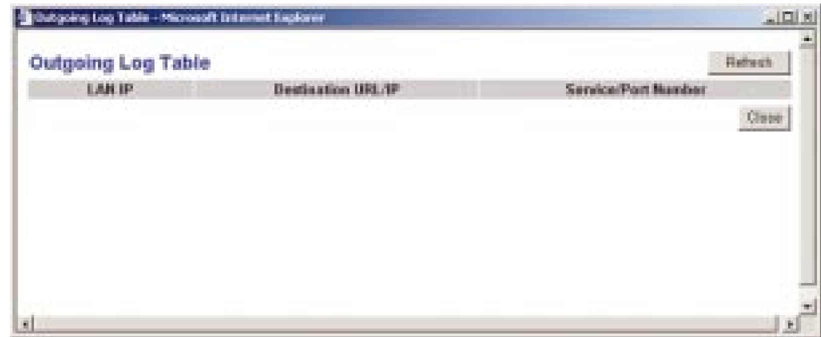


Figure 6-12

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

DHCP

The *DHCP* screen allows you to configure the settings for the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network.

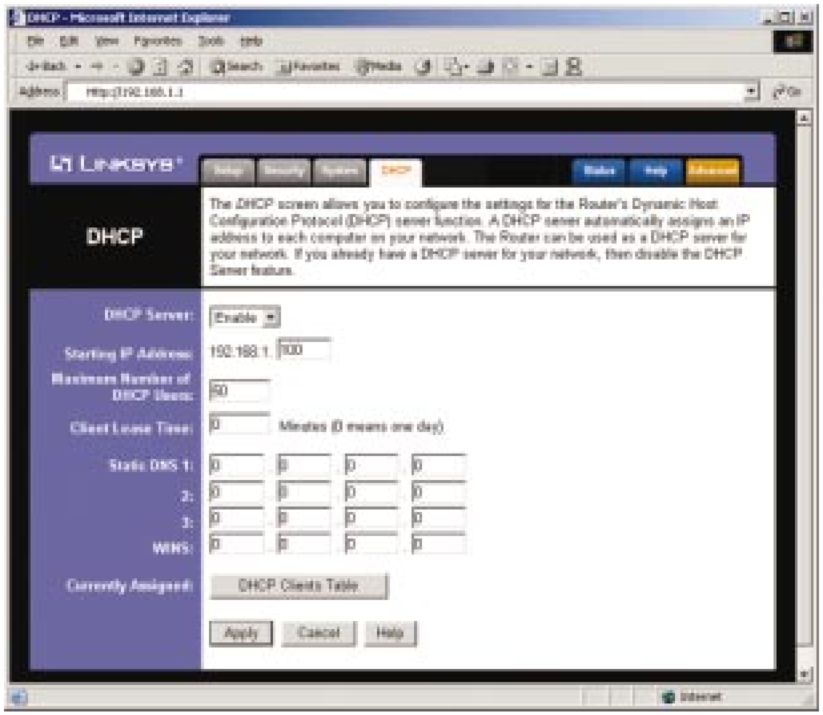


Figure 6-13

If you choose to enable the Router's DHCP server option, you must configure all of your network PCs to connect to a DHCP server (the Router), and make sure there is no other DHCP server on your network.

DHCP Server DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then click the **Disable** radio button (no other DHCP features will be available).

Starting IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is **192.168.1.1**, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default Starting IP Address is **192.168.1.100**.

Number of DHCP Users (Optional) Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

Static DNS 1-3 The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that IP Address in one of these fields. You can type up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Currently Assigned: DHCP Clients Table Click the **DHCP Clients Table** button to view the list of PCs that are given IP addresses by the Router (see Figure 6-14). For each PC, the list shows the Client Hostname, IP Address, MAC Address, and and the amount of DHCP client lease time left. Click the **Refresh** button to display the most current information.

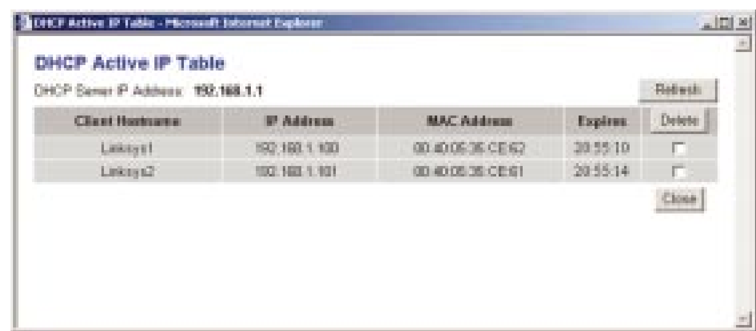


Figure 6-14

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Status

The *Status* screen displays the Router's current status and configuration. All information is read-only.

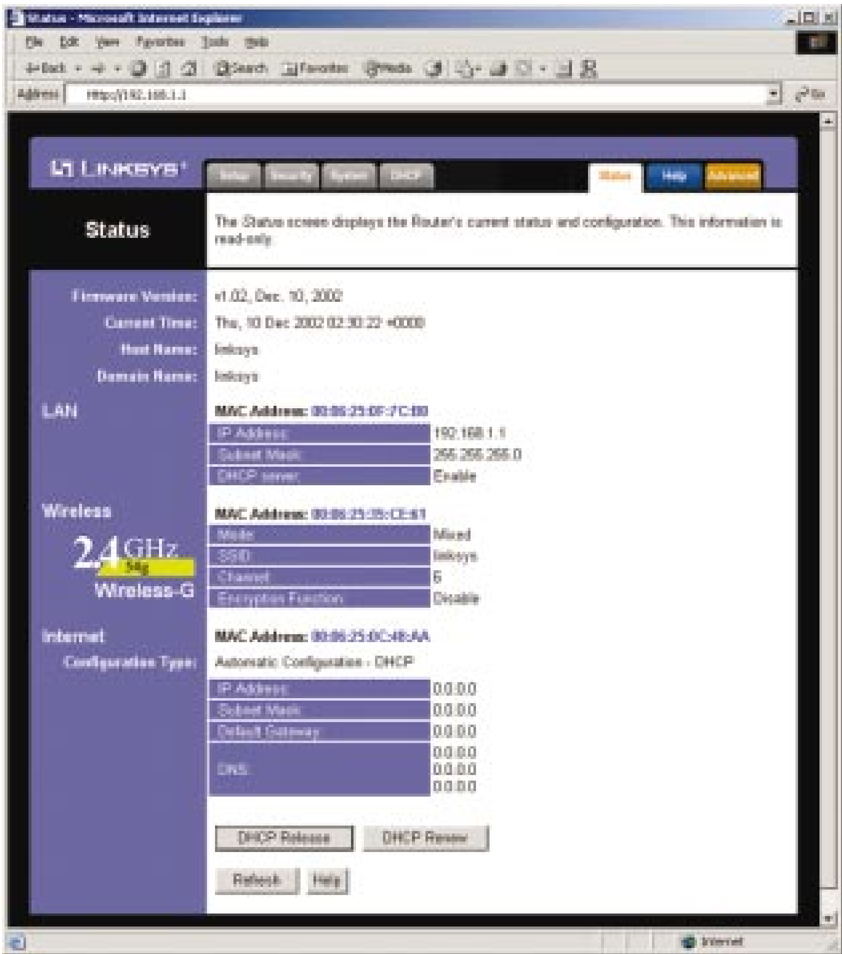


Figure 6-15



Note: The information provided and buttons available may vary depending on the Router's settings.

Firmware Version The version number of the firmware currently installed is displayed here.

Current Time The current date and time are displayed here.

Host Name The Host Name is the name of the Router. This entry is necessary for some ISPs.

Domain Name The Domain Name is the name of the Router's domain. This entry is necessary for some ISPs.

LAN

MAC Address The MAC Address of the LAN interface is displayed here.

IP Address and Subnet Mask The current IP Address and Subnet Mask of the Router, as seen by users on your local area network (LAN), are displayed here.

DHCP Server The status of the Router's DHCP server function is displayed here.

Wireless 2.4GHz, 54g, Wireless-G

MAC Address The MAC Address of the wireless interface is displayed here.

Mode The Mode of the wireless network is displayed here.

SSID The SSID of the wireless network is displayed here.

Channel The Channel of the wireless network is displayed here.

Encryption Function The status of the WEP encryption is displayed here.

Internet

MAC Address The MAC Address of the Internet interface is displayed here.

Configuration Type The type of Internet connection is displayed here.

IP Address, Subnet Mask, and Default Gateway The Router's IP Address, Subnet Mask, and Default Gateway Address, as seen by external users on the Internet, are displayed here.

DNS The DNS (Domain Name System) IP Addresses currently used by the Router are shown here. Multiple DNS IP settings are common. In most cases, the first available DNS entry is used.

DHCP Release Click the **DHCP Release** button to delete the Router's current Internet IP address.

DHCP Renew Click the **DHCP Renew** button to get a new Internet IP address for the Router.

To update the Router's status information, click the **Refresh** button. To get more information about the features, click the **Help** button.

Help

The *Help* screen offers links to all of the Router's technical support resources and the application that upgrades the Router's firmware. For additional information about each screen of the web-based utility, click the appropriate link on the lefthand side of the *Help* screen.

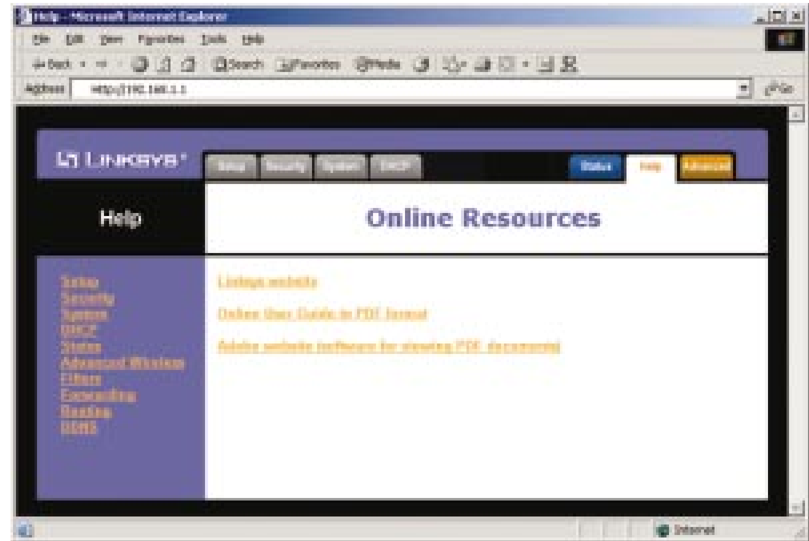


Figure 6-16

Linksys Website Clicking this link will take you to Linksys's website, *www.linksys.com*, provided you are connected to the Internet.

Online User Guide in PDF Format and Adobe Website Clicking the **Online User Guide in PDF format** link opens the Router's User Guide. The User Guide is in Adobe Acrobat Portable Document File (.pdf) format, so you need the Adobe Acrobat Reader to view it. If you do not have the Acrobat Reader, click the **Adobe website** link to download it.

Advanced Tabs

The following instructions are for advanced users or users whose setup needs require special configuration. When you click the **Advanced** tab, you will be able to set up these features. There are five additional tabs available.

Advanced Wireless - Allows you to customize data transmission settings for your wireless network.

Filters - Enables you to set up filters that block or allow specific kinds of Internet usage.

Port Forwarding - Lets you set up public services on your network, such as an ftp server, mail server, or web server.

Routing - Enables you to configure the routing mode and settings of the Router.

DDNS - Allows you to enable the Dynamic Domain Name System (DDNS) feature, so a fixed domain name can be assigned to a dynamic Internet IP address.

If you need to access the basic configuration tabs, click the **Setup** tab.

Advanced Wireless

The *Advanced Wireless* screen allows you to customize data transmission settings. In most cases, the advanced wireless settings on this screen should remain at their default values.

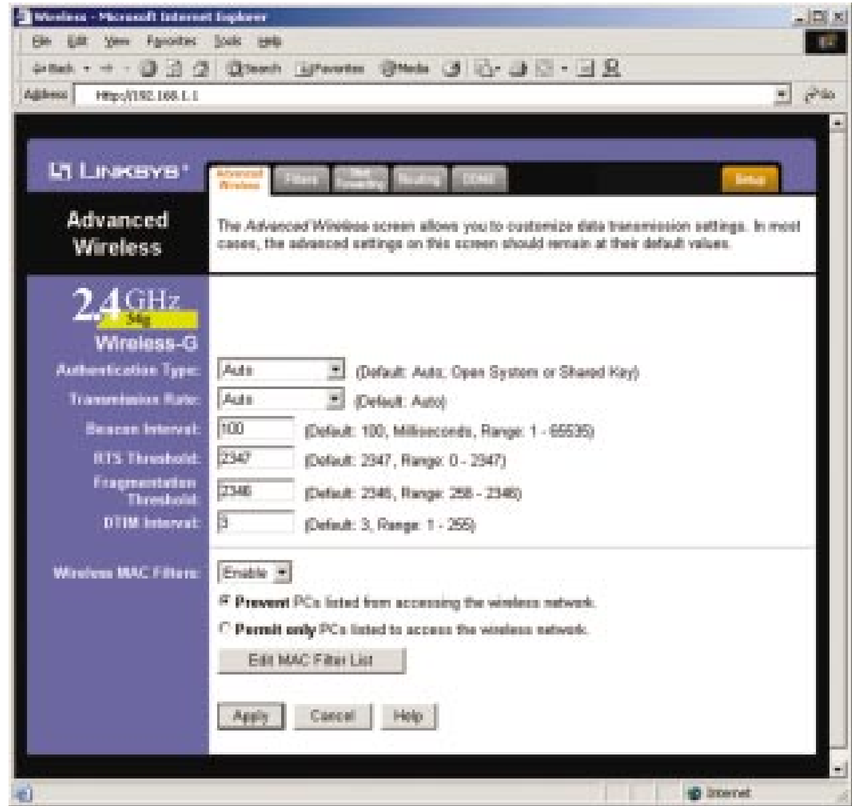


Figure 6-17

Authentication Type The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. For Shared Key authentication, the sender and recipient use a WEP key for authentication. If you want to use only Shared Key authentication, then select **Shared Key**.

Transmission Rate The default setting is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, Auto, to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client.

Beacon Interval The default value is **100**. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

RTS Threshold This value should remain at its default setting of **2347**. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Fragmentation Threshold This value should remain at its default setting of **2346**. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

DTIM Interval The default value is **3**. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

Wireless MAC Filters The Wireless MAC Filters feature allows you to control which wireless-equipped PCs may or may not communicate with the Router-depending on their MAC addresses. To disable the Wireless MAC Filters feature, keep the default setting, **Disable**. To set up a filter, click **Enable**, and follow these instructions:

1. If you want to block specific wireless-equipped PCs from communicating with the Router, then keep the default setting, **Prevent PCs listed from accessing the wireless network**. If you want to allow specific wireless-equipped PCs to communicate with the Router, then click the radio button next to *Permit only PCs listed to access the wireless network*.

2. Click the **Edit MAC Filter List** button. Enter the appropriate MAC addresses into the *MAC* fields (see Figure 6-18).

Note: For each *MAC* field, the MAC address should be entered in this format: xxxxxxxxxxxx (the x's represent the actual characters of the MAC address).

3. Click the **Apply** button to save your changes. Click the **Cancel** button to cancel your unsaved changes. Click the **Close** button to return to the *Advanced Wireless* screen without saving changes.

4. On the *MAC Address Filter List* screen, click the **Wireless Client MAC List** button to view a list of the wireless-equipped PCs (see Figure 6-19).

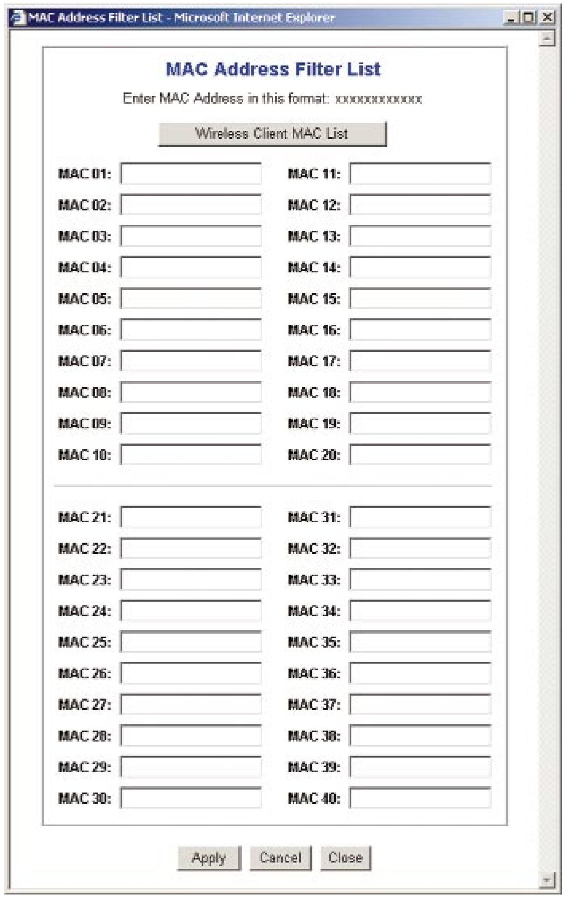


Figure 6-18

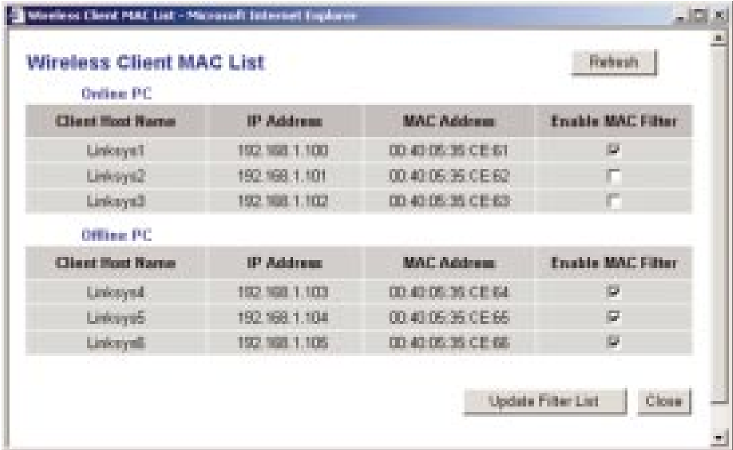


Figure 6-19

For each PC, the list shows—in real time—the Client Host Name, IP Address, MAC Address, and *Enable MAC Filter* option. To enable the MAC address filter for a specific PC, click its **Enable MAC Filter** box. To disable the MAC address filter for a specific PC, uncheck its **Enable MAC Filter** box.

5. Click the **Refresh** button to display the most current information. Click the **Update Filter List** button to update the MAC Address Filter List and return to the MAC Address Filter List screen. Click the **Close** button to return to the *MAC Address Filter List* screen without saving any changes.

6. On the *MAC Address Filter List* screen, click the **Apply** button to save your changes to the MAC Address Filter List. Click the **Cancel** button to cancel your unsaved changes. Click the **Close** button to return to the *Advanced Wireless* screen without saving your changes to the MAC Address Filter List.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Filters

The *Filters* screen allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific PCs and set up filters by using network port numbers.

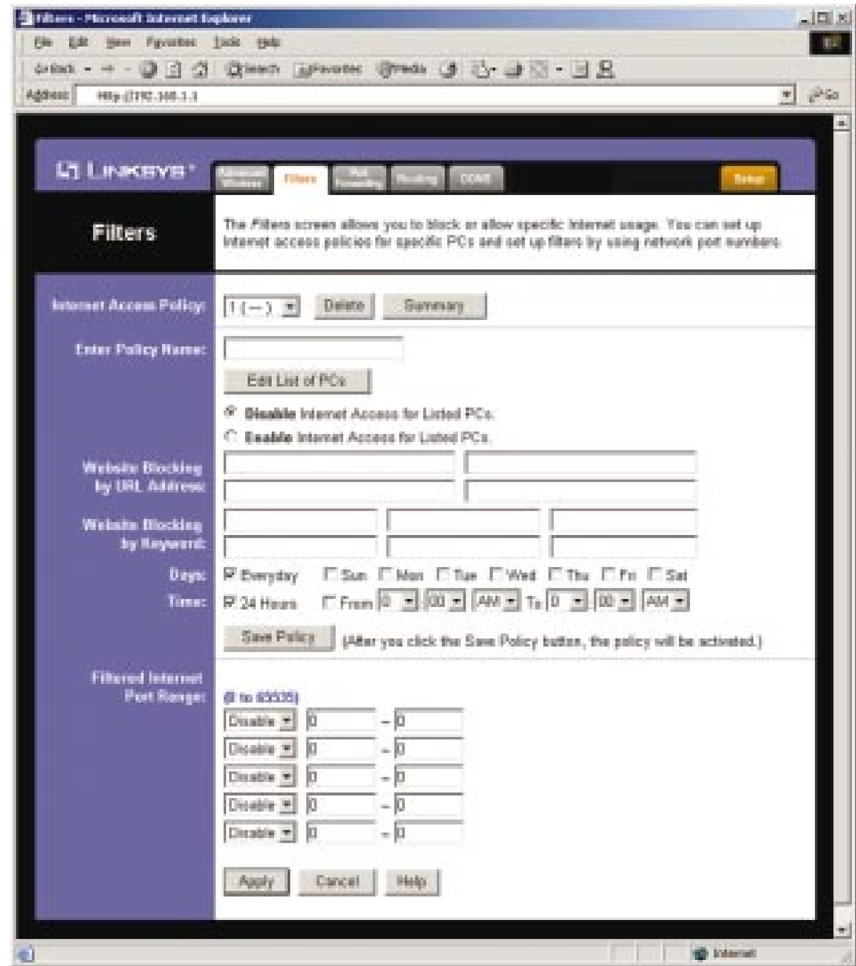


Figure 6-20

Internet Schedule Profile This feature allows you to customize up to ten different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses. For each policy's designated PCs, during the days and time specified, the Router can do one or more of the following:

• block or allow Internet access
• block websites with specific URL addresses
• block websites that use specific keywords in their URL addresses.

To create or edit a policy, follow these instructions:
Then follow these instructions:

1. Select the policy's number (1-10) in the drop-down menu.

2. Enter a name in the *Enter Profile Name* field.

3. Click the **Edit List of PCs** button.

4. On the *List of PCs* screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the *IP* fields. If you have a range of IP addresses to filter, complete the appropriate *IP Range* fields. Enter the appropriate MAC addresses into the *MAC* fields.

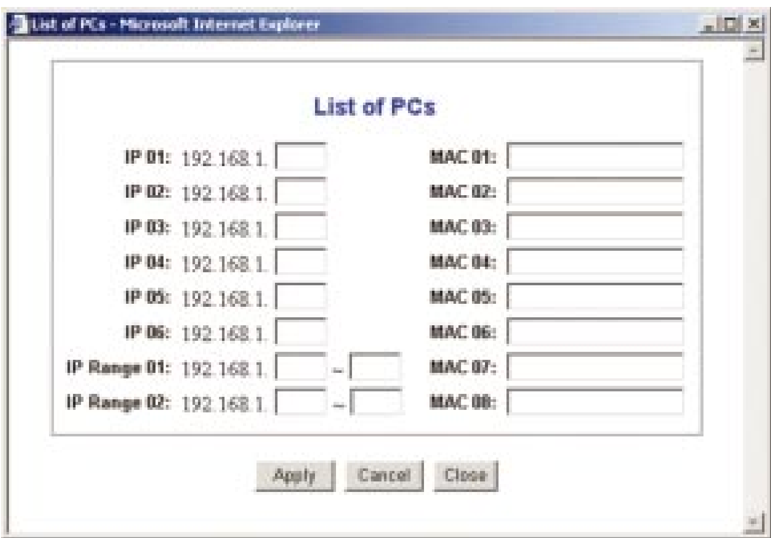


Figure 6-21

5. Click the **Apply** button to save your changes. Click the **Cancel** button to cancel your unsaved changes. Click the **Close** button to return to the *Filters* screen.

6. If you want to block the listed PCs from Internet access during the designated days and time, then keep the default setting, **Disable Internet Access for Listed PCs**. If you want to allow the listed PCs to have Internet access during the designated days and time, then click the radio button next to *Enable Internet Access for Listed PCs*.

7. If you want to block websites with specific URL addresses, enter each URL address in a *Website Blocking by URL Address* field. You can enter up to four URL addresses.

8. If you want to block websites that use specific keywords as part of their URL addresses, enter each keyword in a *Website Blocking by Keyword* field. You can enter up to six keywords.

9. Set the days when access will be filtered. Select **Everyday** or the appropriate days of the week.

10. Set the time when access will be filtered. Select **24 Hours**, or check the box next to *From* and use the drop-down boxes to designate a specific time period.

11. Click the **Save Policy** button to save your changes and activate the Policy. Click the **Cancel** button to cancel your unsaved changes.

12. To create or edit additional policies, repeat steps 1-11.

Delete To delete an Internet Access Policy, select the policy's number, and click the **Delete** button.

Summary To see a summary of all the policies, click the **Summary** button. The *Internet Policy Summary* screen will show each policy's Number, Policy Name, Days, and Time of Day. To delete a policy, click its box, and then click the **Delete** button. Click the **Close** button to return to the *Filters* screen.

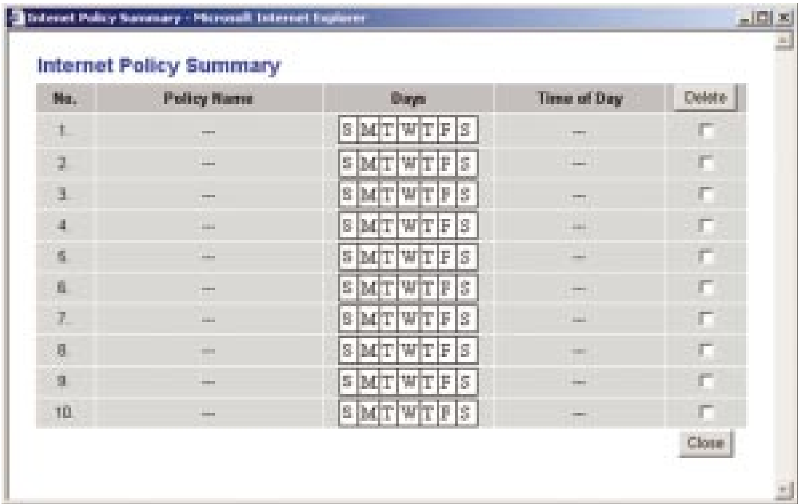


Figure 6-22

Filtered Internet Port Range To filter users by network port number, select **Both**, **TCP**, or **UDP**, depending on which protocols you want to filter. Then enter the port numbers you want to filter into the port number fields. PCs connected to the Router will no longer be able to access any port number listed here. To disable a filter, select **Disable**.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Port Forwarding

The *Port Forwarding* screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

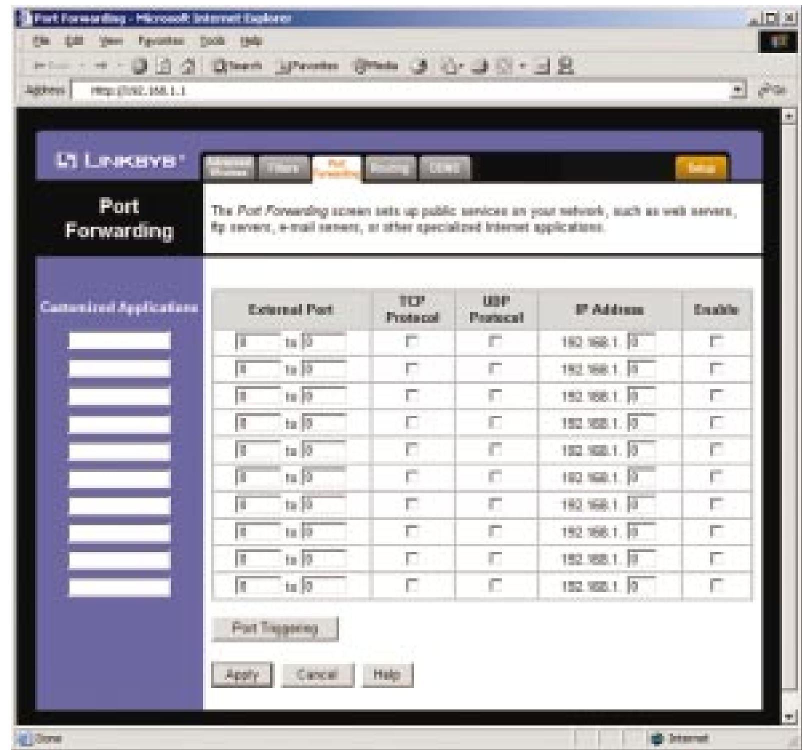


Figure 6-23

When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate PC. Any PC whose port is being forwarded must have its DHCP client function disabled and must have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Note: For each *MAC* field, the MAC address should be entered in this format: xx:xx:xx:xx:xx:xx (the x's represent the actual characters of the MAC address).

The following table shows the typical port forwarding settings for common Internet applications.

Application	External Port	TCP	UDP
FTP	21	•	
Telnet	23	•	
SMTP	25	•	
DNS	53		•
TFTP	69		•
Finger	79	•	
HTTP	80	•	
POP3	110	•	
NNTP	119	•	
SNMP	116		•

Customized Applications In the field provided, enter the name you wish to give each application.

External Port For each application, enter the number of the External Ports (the port numbers seen by users on the Internet) in the appropriate fields. (To find out the port range, check your application's documentation.) If there is only one External Port, enter its number in both External Port fields.

TCP Protocol Click this checkbox if you want to forward the data transmissions that use the TCP protocol.

UDP Protocol Click this checkbox if you want to forward the data transmissions that use the UDP protocol.

IP Address For each application, enter the IP Address of the PC running the specific application.

Enable Click the Enable checkbox to enable port forwarding for the relevant application.

Port Triggering Port Triggering is used for special Internet applications whose outgoing ports differ from the incoming ports. For this feature, the Router will watch outgoing data for specific port numbers. The Router will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules. Click the **Port Triggering** button to set up triggered ports, and follow these instructions:

1. Enter the Application Name of the trigger (see Figure 6-24).

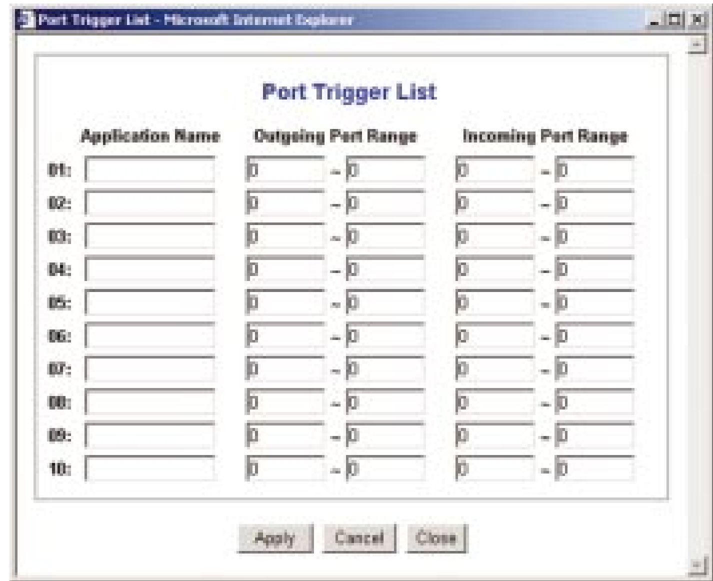


Figure 6-24

2. Enter the Outgoing Port Range used by the application. Check with the Internet application for the port number(s) needed.

3. Enter the Incoming Port Range used by the application. Check with the Internet application for the port number(s) needed.

4. Click the **Apply** button to save your changes. Click the **Cancel** button to cancel your unsaved changes. Click the **Close** button to return to the *Port Forwarding* screen.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Routing

On the *Routing* screen, you can set the routing mode of the Router. Gateway mode is recommended for most users.



Figure 6-25

> **Note:** The *Routing* screen and available features will vary depending on which mode you select.

Operating Mode Choose the correct working mode. Keep the default setting, **Gateway**, if the Router is hosting your network's connection to the Internet (recommended for most users). Select **Router** if the Router exists on a network with other routers.

Dynamic Routing (RIP) Dynamic Routing enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with other routers. The Router determines the network packets' route based on the fewest number of hops between the source and destination. To enable the Dynamic Routing feature for the WAN side, select **WAN**. To enable this feature for the LAN and wireless side, select **LAN & Wireless**. To enable

the feature for both the WAN and LAN (including wireless), select **Both**. To disable the Dynamic Routing feature for all data transmissions, keep the default setting, **Disable**. (This feature is not available in Gateway mode.)

Static Routing A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To set up a static route between the Router and another network, follow these instructions:

1. Select a number from the *Static Routing* drop-down list.

2. Enter the following data:

   - **Destination IP Address -** The Destination IP Address is the address of the network or host to which you want to assign a static route.

   - **Subnet Mask -** The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

   - **Gateway -** This is the IP address of the gateway device that allows for contact between the Router and the network or host.

3. Depending on where the Destination IP Address is located, select **LAN & Wireless** or **WAN** from the *Interface* drop-down menu.

4. To save your changes, click the **Apply** button. To cancel your changes, click the **Cancel** button.

5. For additional static routes, repeat steps 1-4.

Delete This Entry To delete a static route entry, follow these instructions:

1. From the *Static Routing* drop-down list, select the entry number of the static route.

2. Click the **Delete This Entry** button.

3. To save a deletion, click the **Apply** button. To cancel an unsaved deletion, click the **Cancel** button.

Show Routing Table Click the **Show Routing Table** button to view all of the valid dynamic and static route entries in use (see Figure 6-26). The Destination IP address, Subnet Mask, Gateway, and Interface information are displayed for each entry. Click the **Refresh** button to display the most up-to-date data. Click the **Close** button to return to the *Routing* screen.

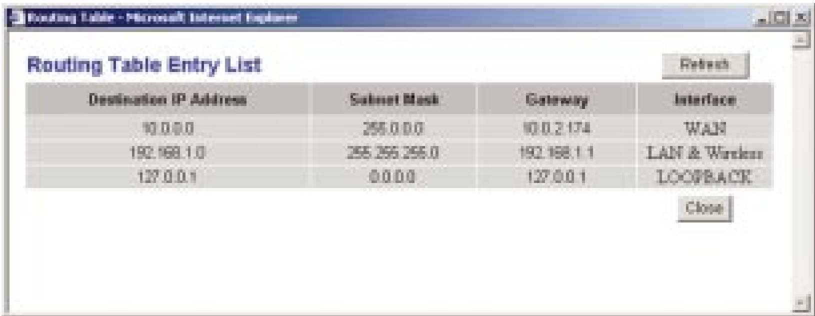


Figure 6-26

- **Destination IP Address** - The Destination IP Address is the address of the network or host to which the static route is assigned.

- **Subnet Mask** - The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

- **Gateway** - This is the IP address of the gateway device that allows for contact between the Router and the network or host.

- **Interface** - This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (internal wired and wireless networks), the **WAN** (Internet), or **Loopback** (a dummy network in which one PC acts like a network-necessary for certain software programs).

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before you can use this feature, you need to sign up for DDNS service at *www.dyndns.org*, a DDNS service provider.

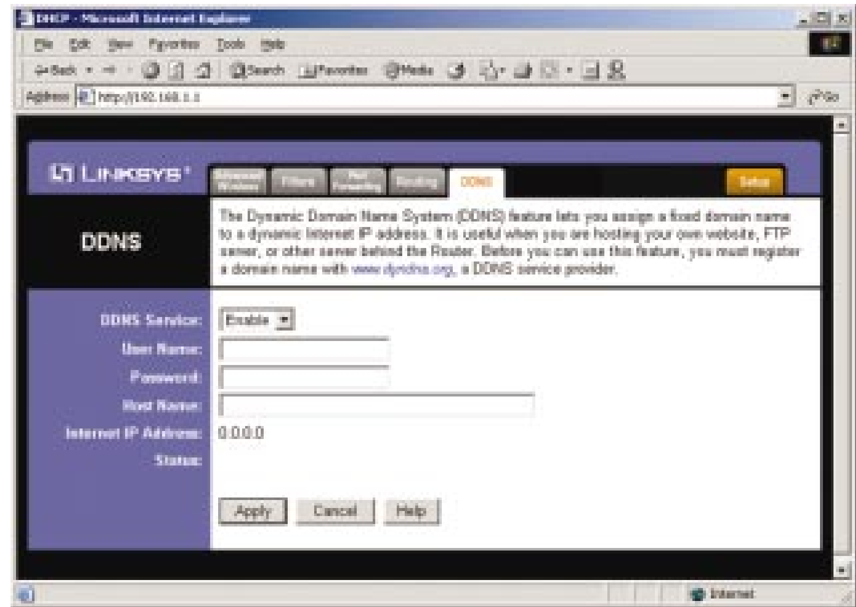


Figure 6-27

DDNS Service To disable DDNS Service, keep the default setting, **Disable**. To enable DDNS Service, follow these instructions:

1. Sign up for DDNS service at *www.dyndns.org*, and write down your User Name, Password, and Host Name information.

2. On the *DDNS* screen, select **Enable**.

3. Complete the *User Name*, *Password*, and *Host Name* fields.

4. To save your new settings, click the **Apply** button. To cancel your changes, click the **Cancel** button.

Internet IP Address The Router's current Internet IP Address is displayed here.

Status The status of the DDNS service connection is displayed here.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Appendix A: Troubleshooting

Common Problems and Solutions

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

1. I need to set a static IP address on a PC.

You can assign a static IP address to a PC by performing the following steps:

For Windows 98 and Me:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.

B. In *The following network components are installed* box, select the **TCP/IP->** associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the **Properties** button.

C. In the *TCP/IP properties* window, select the **IP address** tab, and select **Specify an IP address**. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Make sure that each IP address is unique for each PC or network device.

D. Click the **Gateway** tab, and in the *New Gateway* prompt, enter **192.168.1.1**, which is the default IP address of the Router. Click the **Add** button to accept the entry.

E. Click the **DNS** tab, and make sure the **DNS Enabled** option is selected. Enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Enter the **DNS entry** provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.

F. Click the **OK** button in the *TCP/IP properties* window, and click **Close** or the **OK** button for the Network window.

G. Restart the computer when asked.

For Windows 2000:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
B. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
C. In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Select **Use the following IP address** option.
D. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
E. Enter the Subnet Mask, **255.255.255.0**.
F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
G. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the **Preferred DNS server** and **Alternative DNS server** (provided by your ISP). Contact your ISP or go on its website to find the information.
H. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
I. Restart the computer if asked.

For Windows NT 4.0:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
B. Click the **Protocol** tab, and double-click **TCP/IP Protocol**.
C. When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter.
D. Select **Specify an IP address**, and enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
E. Enter the Subnet Mask, **255.255.255.0**.
F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
G. Click the **DNS** tab, and enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Under DNS Service Search Order, click the **Add** button. Enter the **DNS IP address** in the *DNS Server* field, and click the **Add** button. Repeat this action for all DNS IP addresses given by your ISP.
H. Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.
I. Restart the computer if asked.

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

A. Click **Start** and **Control Panel**.
B. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
C. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
D. In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
E. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
F. Enter the Subnet Mask, **255.255.255.0**.
G. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
H. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the **Preferred DNS server** and **Alternative DNS server** (provided by your ISP). Contact your ISP or go on its website to find the information.
I. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window. Click the **OK** button in the *Local Area Connection Properties* window.

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:
Refer to "Chapter 4: Configure the PCs" for details. Make sure **Obtain IP address automatically** is selected in the settings.

For Windows NT 4.0:
- Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
- Click the **Protocol** tab, and double-click on **TCP/IP Protocol**.
- When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter and set it for **Obtain an IP address from a DHCP server**.
- Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.
- Restart the computer if asked.

B. Open a command prompt.
  - For **Windows 98** and **Me**, please click **Start** and **Run**. In the *Open* field, type in **command**. Press the **Enter** key or click the **OK** button.
  - For **Windows NT, 2000,** and **XP**, please click **Start** and **Run**. In the Open field, type **cmd**. Press the **Enter** key or click the **OK** button.

C. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.
  - If you get a reply, the computer is communicating with the Router.
  - If you do NOT get a reply, please check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.

D. In the command prompt, type **ping** *followed by your Internet or WAN IP address* and press the **Enter** key. The Internet or WAN IP Address can be found on the *Status* screen of the Router's web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.
  - If you get a reply, the computer is connected to the Router.
  - If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

E. In the command prompt, type **ping www.yahoo.com** and press the **Enter** key.
  - If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
  - If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. I am not getting an IP address on the Internet with my Internet connection.

A. Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.

B. If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix D: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of "Chapter 6: The Router's Web-based Utility" for details.

C. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 6: The Router's Web-based Utility" for details on Internet connection settings.

D. Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.

E. Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's web-based utility shows a valid IP address from your ISP.

F. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the *Status* tab of the Router's web-based utility to see if you get an IP address.

4. I am not able to access the Setup page of the Router's web-based utility.

A. Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Router.

B. Refer to "Appendix D: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.

C. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."

D. Refer to "Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

5. I can't get my Virtual Private Network (VPN) working through the Router.

Access the Router's web interface by going to **http://192.168.1.1** or the **IP address** of the Router, and go to the **Security** tab. Make sure you have IPsec pass-through and/or PPTP pass-through enabled.

VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions *may* be possible, depending on the specifics of your VPNs.

VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.

Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the *Setup* tab

of the web interface. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.

Check the Linksys website for more information at *www.linksys.com*.

6. I need to set up a server behind my Router and make it available to the public.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed. Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.

A. Access the Router's web-based utility by going to **http://192.168.1.1** or the **IP address** of the Router. Go to the **Advanced => Port Forwarding** tab.
B. Enter any **name** you want to use for the Customized Application.
C. Enter the **External Port range** of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
D. Check the **protocol** you will be using, TCP and/or UDP.
E. Enter the **IP address** of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
F. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
Web server	80 to 80	X	X	192.168.1.100	X
FTP server	21 to 21	X		192.168.1.101	X
SMTP (outgoing)	25 to 25	X	X	192.168.1.102	X
POP3 (incoming)	110 to 110	X	X	192.168.1.102	X

When you have completed the configuration, click the **Apply** button.

7. I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

A. Access the Router's web interface by going to **http://192.168.1.1** or the **IP address** of the Router. Go to the **Advanced => Port Forwarding** tab.
B. Enter any **name** you want to use for the Customized Application.
C. Enter the **External Port range** of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
D. Check the **protocol** you will be using, TCP and/or UDP.
E. Enter the **IP address** of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
F. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
UT	7777 to 27900	X	X	192.168.1.100	X
Halflife	27015 to 27015	X	X	192.168.1.105	X
PC Anywhere	5631 to 5631		X	192.168.1.102	X
VPN IPSEC	500 to 500		X	192.168.1.100	X

When you have completed the configuration, click the **Apply** button.

8. I can't get the Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.) Follow these steps to set DMZ hosting:

A. Access the Router's web-based utility by going to **http://192.168.1.1** or the **IP address** of the Router. Go to the **Advanced => Port Forwarding** tab.
B. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
C. Go to the **Setup => Security** tab.
D. Select **Enable** next to *DMZ*. In the *DMZ Host IP Address* field, enter the **IP address** of the computer you want exposed to the Internet. This will bypass the NAT technology for that computer. Please refer to "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

Once completed with the configuration, click the **Apply** button.

9. I forgot my password, or the password prompt always appears when I am saving settings to the Router.

Reset the Router to factory default by pressing the **Reset** button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

A. Access the Router's web-based utility by going to **http://192.168.1.1** or the **IP address** of the Router. Enter the default password **admin**, and click the **Security** tab.
B. Enter a **different password** in the *Router Password* field, and enter the same password in the second field to confirm the password.
C. Click the **Apply** button.

10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Internet Options**.
B. Click the **Connections** tab.
C. Click the **LAN settings** button and remove anything that is checked.
D. Click the **OK** button to go back to the previous screen.
E. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:

A. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
B. Make sure you have **Direct connection to the Internet** selected on this screen.
C. Close all the windows to finish.

11. To start over, I need to set the Router to factory default.

Hold the **Reset** button for 10 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at *www.linksys.com*. Follow these steps:

A. Go to the Linksys website at **http://www.linksys.com** and download the latest firmware.
B. To upgrade the firmware, follow the steps in the System section found in "Chapter 6: The Router's Web-based Utility."

13. The firmware upgrade failed, and/or the Diag LED is flashing.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Diag LED stop flashing:

A. If the firmware upgrade failed, use the **TFTP** program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
B. Set a **static IP address** on the PC; refer to “Problem #1, I need to set a static IP address.” Use the following IP address settings for the computer you are using:

    IP Address: 192.168.1.50
    Subnet Mask: 255.255.255.0
    Gateway: 192.168.1.1

C. Perform the upgrade using the TFTP program or the Router’s web-based utility through its *System* tab.

14. My DSL service’s PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to “keep alive” the connection. This may not always work, so you may need to re-establish connection periodically.

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the **IP address** of the Router.
B. Enter the **password**, if asked. (The default password is **admin**.)
C. On the *Setup* screen, select the option **Keep Alive**, and set the **Redial Period** option at **20** (seconds).
D. Click the **Apply** button.
E. Click the **Status** tab, and click the **Connect** button.
F. You may see the login status display as **Connecting**. Press the **F5** key to refresh the screen, until you see the login status display as **Connected**.
G. Click the **Apply** button to continue.

If the connection is lost again, follow steps E to G to re-establish connection.

15. I can’t access my e-mail, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you are having some difficulties, perform the following steps:

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the **IP address** of the Router.
B. Enter the password, if asked. (The default password is **admin**.)
C. Click the **System** tab.
D. Look for the MTU option, and select **Manual**. In the *Size* field, enter **1492**.
E. Click the **Apply** button to continue.

If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:

    1462
    1400
    1362
    1300

16. The Diag LED stays lit continuously.

- The Diag LED lights up when the device is first powered up. Meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED turns off to show that the system is working fine. If the LED remains lit after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.

- Check if other PCs work. If they do, ensure that your workstation’s IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.

- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

18. The Full/Col LED keeps flickering continuously.
- Check the Category 5 Ethernet network cable and its RJ-45 connectors.
- There may be interference with other network devices. Try removing other PCs or network devices to see if the problem persists. Eliminate each network device one at a time to determine the cause.

Frequently Asked Questions

What is the maximum number of IP addresses that the Router will support?
The Router will support up to 253 IP addresses.

Is IPSec Pass-Through supported by the Router?
Yes, it is a built-in feature that the Router automatically enables.

Where is the Router installed on the network?
In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

Does the Router support IPX or AppleTalk?
No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.

Does the Internet connection of the Router support 100Mbps Ethernet?
The Router's current hardware design supports up to 100Mbps Ethernet on its Internet port; however, the Internet connection speed will vary depending on the speed of your broadband connection. The Router also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.

What is **Network Address Translation** and what is it used for?
Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with low cost Internet accounts, such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Router support any operating system other than Windows 95, Windows 98, Windows Millennium, Windows 2000, Windows NT, or Windows XP?
Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the Router support ICQ send file?
Yes, with the following fix: click **ICQ menu -> preference -> connections tab->**, and check **I am behind a firewall or proxy**. Then set the firewall time-out to **80** seconds in the firewall setting. The Internet user can then send a file to a user behind the Router.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?
If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get *Half-Life: Team Fortress* to work with the Router?
The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. *One problem:* Version 1.0.1.6 won't let multiple computers with the

same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

How can I block corrupted FTP downloads?

If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?

Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at *www.linksys.com* for more information.

If all else fails in the installation, what can I do?

Reset the Router by holding down the reset button until the Diag LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, *www.linksys.com*.

How will I be notified of new Router firmware upgrades?

All Linksys firmware upgrades are posted on the Linksys website at *www.linksys.com*, where they can be downloaded for free. To upgrade the Router's firmware, use the *System* tab of the Router's web-based utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Will the Router function in a Macintosh environment?

Yes, but the Router's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Router. What can I do?

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that

your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

What is DMZ Hosting?

Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter."

If DMZ Hosting is used, does the exposed user share the public IP with the Router?

No.

Does the Router pass PPTP packets or actively route PPTP sessions?

The Router allows PPTP packets to pass through.

Is the Router cross-platform compatible?

Any platform that supports Ethernet and TCP/IP is compatible with the Router.

How many ports can be simultaneously forwarded?

Theoretically, the Router can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

Does the Router replace a modem? Is there a cable or DSL modem in the Router?

No, the Router must work in conjunction with a cable or DSL modem.

Which modems are compatible with the Router?

The Router is compatible with virtually any cable or DSL modem that supports Ethernet.

What are the advanced features of the Router?

The Router's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.

What is the maximum number of VPN sessions allowed by the Router?

The maximum number depends on many factors. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions *may* be possible, depending on the specifics of your VPNs.

How can I check whether I have static or DHCP IP Addresses?
Consult your ISP to obtain this information.

How do I get mIRC to work with the Router?
Under the *Port Forwarding* tab, set port forwarding to 113 for the PC on which you are using mIRC.

Can the Router act as my DHCP server?
Yes. The Router has DHCP server software built-in.

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

What is the IEEE 802.11b standard?
It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11b functions:
- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is ad-hoc mode?
When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.

What is infrastructure mode?
When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is roaming?
Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is ISM band?
The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?
Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not

tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Will the information be intercepted while it is being transmitted through the air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I avoid interference?

If you are using the Router and one or more Access Points in close proximity to one another, and they are set on the same channel, interference will be generated. To avoid interference, be sure to set the Router and all Access Points to different channels (frequencies); in other words, assign a unique channel to the Router and each Access Point.

How do I reset the Router?

Press the **Reset** button on the back panel for about ten seconds. This will reset the Router to its default settings.

How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Router and a wireless PC will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Router and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.

WEP is probably enabled on the Router, but not on your wireless adapter (or vice versa). Verify that the same WEP keys and levels (64 or 128) are being used on all nodes of your wireless network.

How many channels/frequencies are available with the Router?

There are eleven available channels, ranging from 1 to 11 (in North America).

If your questions are not addressed here, refer to the Linksys website, *www.linksys.com*.

Appendix B: How to Ping Your ISP's E-mail & Web Addresses

Virtually all Internet addresses are configured with words or characters (e.g., *www.linksys.com*, *www.yahoo.com*, etc.) In actuality, however, these Internet addresses are assigned to IP addresses, which are the true addresses on the Internet. For example, *www.yahoo.com* is 66.218.71.87 (this IP address may change). Type it into your web browser and you will wind up at the Linksys home page every time. There are servers that translate the URL to an IP address; this is called the Domain Name System (DNS).

IP and web addresses, however, can sometimes be long and hard to remember. Because of this, certain ISPs will shorten their server addresses to single words or codes on their users' web browser or e-mail configurations. If your ISP's e-mail and web server addresses are configured with single words (*www*, *e-mail*, *home*, *pop3*, etc.) rather than whole Internet addresses or IP addresses, the Router may have problems sending or receiving mail and accessing the Internet. This happens because the Router has not been configured by your ISP to accept their abbreviated server addresses.

The solution is to determine the true web addresses behind your ISPs code words. You can determine the IP and web addresses of your ISP's servers by "pinging" them.

Important: If you don't have your ISP's web and e-mail IP addresses, you *must* either get them from your ISP or follow these steps *prior* to connecting the Router to your network.

Step One: Pinging an IP Address

The first step to determining your ISP's web and e-mail server address is to ping its IP address.

1. Power on the computer and the cable or DSL modem, and restore the network configuration set by your ISP if you have since changed it.

2. Click **Start** and then **Run**. Type **command** in the **Open** field. This will bring up the DOS window.

3. At the DOS command prompt, type **ping mail** (assuming that the location for which you're trying to find an IP address is configured as *mail*). Press the **Enter** key. Information such as the following data, taken from a ping of Microsoft Network's e-mail server, will be displayed.

```
C:\>ping mail

Pinging mail [24.53.32.4] with 32 bytes of data:

Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128

Ping statistics for 24.53.32.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
   loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure B-1

4. Write down the IP address returned by the ping command (in the example above: 24.53.32.4.). This IP address is the actual IP address of the server *mail*, or any other word or value you have pinged.

Step Two: Pinging for a Web Address

While the IP address returned above would work as your e-mail server address, it may not be permanent. IP addresses change all the time. Web addresses, however, usually don't. Because of this, you're likely to have fewer problems by configuring your system with web addresses rather than IP addresses. Follow the instructions below to find the web address assigned to the IP address you just pinged.

1. At the DOS command prompt, type **ping -a 24.53.32.4**, where 24.53.32.4 is the IP address you just pinged. Information such as the following data will be displayed.

```
C:\>ping -a 24.53.32.4

Pinging mail.msnv3.occa.home.com [24.53.32.4] with
   32 bytes of data:

Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127

Ping statistics for 24.53.32.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
   loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure B-2

2. Write down the web address returned by the ping command. (In the example in Figure C-2, *mail.msnv3.occa.home.com* is the web address.) This web address is the web address assigned to the IP address you just pinged. While the IP address of *mail* could conceivably change, it is likely that this web address will not.

3. Replace your ISP's abbreviated server address with this extended web address in the corresponding Internet application (web browser, e-mail application, etc.).

Once you have replaced the brief server address with the true server address, the Router should have no problem accessing the Internet through that Internet application.

Appendix C: Configuring Wireless Security

An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode a data transmission, each point in a network must use an identical 64-bit or 128-bit key. Higher encryption levels mean higher levels of security, but due to the complexity of the encryption, they may mean decreased network performance.

You may also have heard the term "40-bit" used in conjunction with WEP encryption. This is simply another term for 64-bit WEP encryption. This level of WEP encryption has been called 40-bit because it uses a 40-bit secret key along with a 24-bit Initialization Vector (40 + 24 = 64). Wireless vendors may use either name. Linksys uses the term "64-bit" when referring to this level of encryption. All wireless devices compliant with the 802.11b standard will support 64-bit WEP.

Note: WEP encryption is an additional data security measure and not essential for router operation; however, Linksys recommends the use of WEP encryption.

Make sure your wireless network is functioning before attempting to configure WEP encryption.

In addition to enabling WEP, Linksys also recommends the following security implementations:
- Change the SSID from the default "linksys"
- Change the SSID on a regular basis
- Change the WEP key regularly
- Enable wireless MAC address filtering (see the "Advanced Wireless" section of "Chapter 6: The Router's Web-Based Utility")

For instructions on how to configure the WEP settings of your PC's wireless adapter, refer to your wireless adapter's documentation. To configure the Router's WEP settings, follow these instructions:

1. On the *Setup* tab of the Router's web-based utility, click the **Enable** radio button next to *WEP*. Then click the **Edit WEP Settings** button.

2. You will see the *2.4GHz, 54g, Wireless-G (WEP)* screen (Figure C-1). Next to ***Default Transmit Key***, select which WEP key (1-4) will be used when the Router sends data. Make sure the receiving device is using the same key.

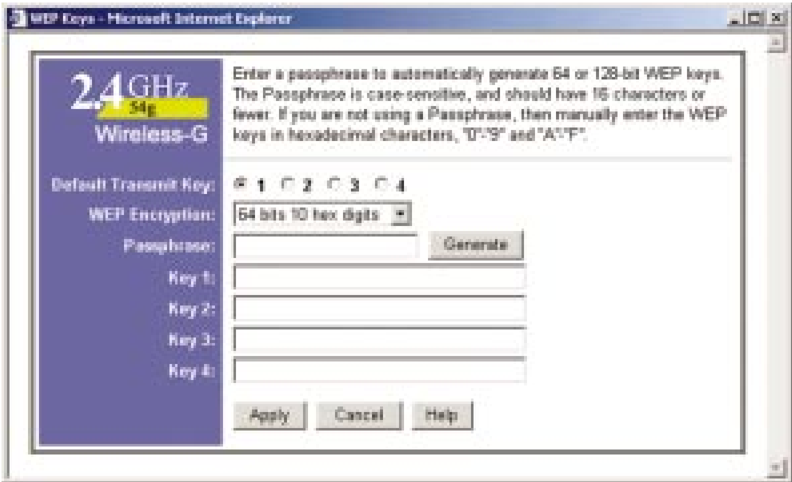


Figure C-1

3. For the ***WEP Encryption*** drop-down box, select the level of WEP encryption you wish to use, **64-bit 10 hex digits** or **128-bit 26 hex digits**. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

4. Instead of manually entering WEP keys, you can enter a Passphrase in the *Passphrase* field. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, enter the WEP key manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

Note: All Wireless-G and 802.11b devices in your network must use the same Passphrase or WEP key.

5. WEP keys enable you to create an encryption scheme for wireless LAN transmissions. If you are not using a Passphrase, then manually enter a set of values in each *Key* field. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.)

   If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F".

6. Check all the values, and click the **Apply** button to save your WEP settings and return to the *Setup* screen. To cancel any changes you've entered on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your Ethernet adapter to do either MAC address filtering or MAC address cloning for the Router and ISP. You can also find the IP address of your computer's Ethernet adapter. The IP address is used for filtering, forwarding, and DMZ. Follow the steps in this appendix to find the MAC address or IP address for your adapter in Windows 95, 98, Me, NT, 2000, and XP.

For Windows 95, 98, and Me:

1. Click on **Start** and **Run**. In the Open field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.

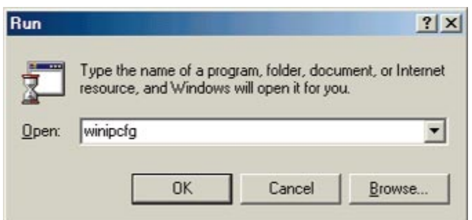


Figure D-1

2. When the IP Configuration window appears, select the Ethernet adapter you are using to connect to the Router via a Category 5 Ethernet network cable.

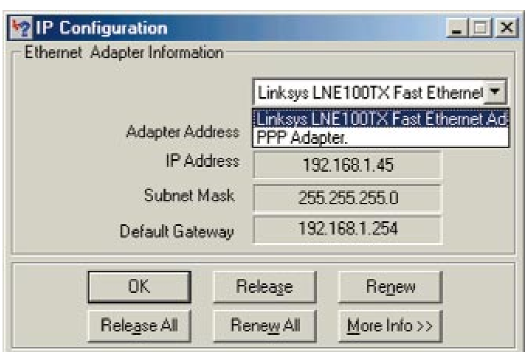


Figure D-2

3. Write down the Adapter Address as shown on your computer screen (see Figure E-3). This is the MAC address for your Ethernet adapter and will be shown as a series of numbers and letters.

   The MAC address/Adapter Address is what you will use for MAC address cloning or MAC filtering.

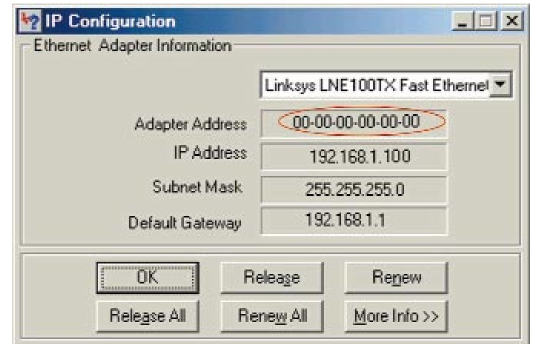


Figure D-3

Write down the IP Address as shown on your computer screen. The example in Figure E-3 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

Note: The MAC address is also called the Adapter Address.

For Windows NT, 2000, and XP:

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.

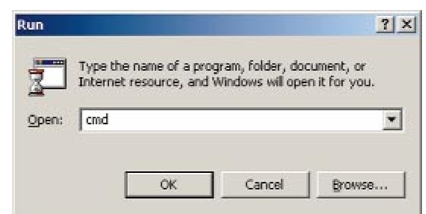


Figure D-4

2. In the command prompt, enter **ipconfig /all**. Then press the **Enter** key.

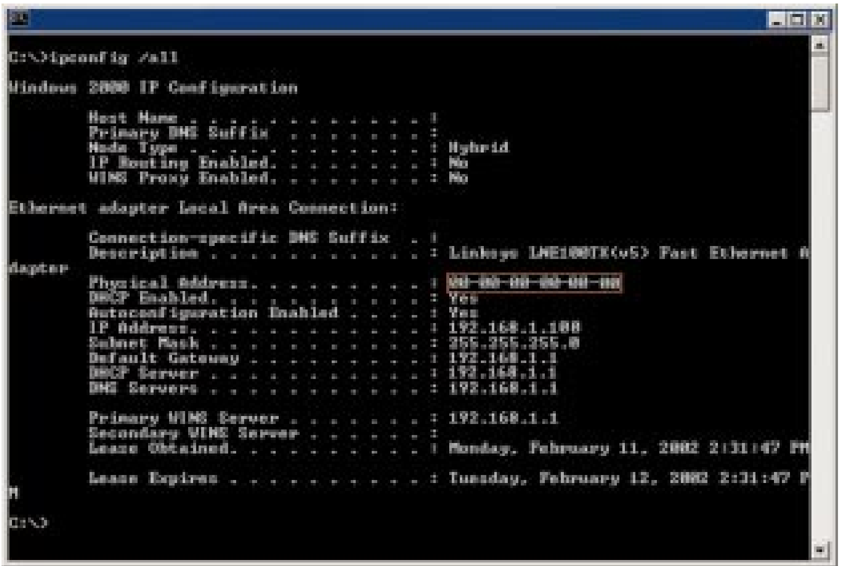


Figure D-5

3. Write down the Physical Address as shown on your computer screen; it is the MAC address for your Ethernet adapter. This will appear as a series of letters and numbers.

   The MAC address/Physical Address is what you will use for MAC address cloning or MAC filtering.

   Note: The MAC address is also called the Physical Address.

   Write down the IP Address as shown on your computer screen. The example in Figure E-5 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

Appendix E: Glossary

10BaseT - An Ethernet standard that uses twisted wire pairs.

100BaseTX - IEEE physical layer specification for 100 Mbps over two pairs of Category 5 UTP or STP wire.

802.11b - One of the IEEE standards for wireless networking hardware. Products that adhere to a specific IEEE standard will work with each other, even if they are manufactured by different companies. The 802.11b standard specifies a maximum data transfer rate of 11Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

802.1g - A proposed, but as yet unratified extension of the IEEE 802.11 standard for wireless networking hardware. The draft 802.11g specifications used by Linksys specify a maximum data transfer rate of 54Mbps using OFDM modulation, an operating frequency of 2.4GHz, backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

Adapter - Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC. In a networked environment, a network interface card (NIC) is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

Ad-hoc Network - An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.

Automatic Fall-back - A feature provided by some wireless products to increase connection reliability. Automatic fall-back enables a device to dynamically shift between various data transfer rates. It works by decreasing the data transfer rate when interference increases, distance increases, and other factors undermine signal strength and quality.

Auto-MDI/MDIX - On a network hub or switch, an auto-MDI/MDIX port automatically senses if it needs to act as a MDI or MDIX port. The auto-MDI/MDIX capability eliminates the need for crossover cables.

Auto-negotiate - To automatically determine the correct settings. The term is often used with communications and networking. For example, Ethernet 10/100 cards, hubs, and switches can determine the highest speed of the node they are connected to and adjust their transmission rate accordingly.

Backbone – The part of a network that connects most of the systems and networks together and handles the most data.

Bandwidth - The transmission capacity of a given facility, in terms of how much data the facility can transmit in a fixed amount of time; expressed in bits per second (bps).

Beacon Interval - A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit – A binary digit. The value—0 or 1—used in the binary numbering system. Also, the smallest form of data.

Boot – To cause the computer to start executing instructions. Personal computers contain built-in instructions in a ROM chip that are automatically executed on startup. These instructions search for the operating system, load it, and pass control to it.

Bottleneck – A traffic slowdown that results when too many network nodes try to access a single node, often a server node, at once.

Bridge - A device that interconnects different networks together.

Broadband - A data-transmission scheme in which multiple signals share the bandwidth of a medium. This allows the transmission of voice, data, and video signals over a single medium. Cable television uses broadband techniques to deliver dozens of channels over one cable.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web or PC. The word “browser” seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

Buffer - A buffer is a shared or assigned memory area used by hardware devices or program processes that operate at different speeds or with different

sets of priorities. The buffer allows each device or process to operate without being held up by the other. In order for a buffer to be effective, the size of the buffer and the algorithms for moving data into and out of the buffer need to be considered by the buffer designer. Like a cache, a buffer is a “midpoint holding place” but exists not so much to accelerate the speed of an activity as to support the coordination of separate activities.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet. Once connected, cable modem users have a continuous connection to the Internet. Cable modems feature asymmetric transfer rates: around 36 Mbps downstream (from the Internet to the computer), and from 200 Kbps to 2 Mbps upstream (from the computer to the Internet).

CAT 5 - ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify “categories” (the singular is commonly referred to as “CAT”) of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 5 cable has a maximum throughput of 100 Mbps and is usually utilized for 100BaseTX networks.

CPU (**C**entral **P**rocessing **U**nit) - The computing part of the computer. Also called the “processor,” it is made up of the control unit and ALU.
CSMA/CD (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection) - The LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and each waits a random amount of time before retrying.

CTS (**C**lear **T**o **S**end) - An RS-232 signal sent from the receiving station to the transmitting station that indicates it is ready to accept data.

Database - A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.

Data Packet - One frame in a packet-switched message. Most data communications is based on dividing the transmitted message into packets. For example, an Ethernet packet can be from 64 to 1518 bytes in length.

Default Gateway - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows a network device with a dynamic Internet IP address to have a fixed host and domain name, such as *myhostname.mydomainname.com*. It is useful when you are hosting your own website, FTP server, or other server behind a router, so people can find your site no matter how often the Internet IP address changes. Using DDNS requires registering with a DDNS service provider on the Internet.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DMZ - (**D**e**M**ilitarized **Z**one) allows one IP address (or computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP address if you want to use DMZ Hosting.

DNS - The Domain Name System (DNS) is the way that Internet domain names are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Domain - A subnetwork comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Download - To receive a file transmitted over a network. In a communications session, download means receive, and upload means transmit.

Driver - A workstation or server software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific NIC, and is installed during the initial installation of a network-compatible client or server operating system.

DSSS (**D**irect-**S**equence **S**pread **S**pectrum) - DSSS generates a redundant bit pattern for all transmitted data. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages.

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

Dynamic Routing - The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Has a transfer rate of 10 Mbps. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

Fast Ethernet - A 100 Mbps technology based on the 10Base-T Ethernet CSMA/CD network access method.

FHSS (**F**requency **H**opping **S**pread **S**pectrum) - FHSS continuously changes (hops) the carrier frequency of a conventional carrier several times per second according to a pseudo-random set of channels. Because a fixed frequency is not used, and only the transmitter and receiver know the hop patterns, interception of FHSS is extremely difficult.

Firewall - A firewall is a set of related programs, located at a network gateway server, that protects the resources of a network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access.

Basically, a firewall, working closely with a router, examines each network packet to determine whether to forward it toward its destination.

Firmware - Code that is written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the Web server using FTP.

FTP includes functions to log onto the network, list directories, and copy files. It can also convert between the ASCII and EBCDIC character codes. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. FTP transfers can also be initiated from within a Web browser by entering the URL preceded with ftp://.

Unlike e-mail programs in which graphics and program files have to be “attached,” FTP is designed to handle binary files directly and does not add the overhead of encoding and decoding the data.

Full Duplex - The ability of a device or line to transmit data simultaneously in both directions.

Gateway – A device that interconnects networks with different, incompatible communications protocols.
Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the “box” and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

Hub - The device that serves as the central location for attaching wires from workstations. Can be passive, where there is no amplification of the signals; or active, where the hubs are used like repeaters to provide an extension of the cable that connects to a workstation.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a Web server and transmit HTML pages to the client browser.

IEEE - The Institute of Electrical and Electronics Engineers. The IEEE describes itself as “the world's largest technical professional society—promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members.”

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and has several large societies in special areas, such as the IEEE Computer Society.

Infrastructure Network - An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at

a corporation scale, or when it is necessary to connect the wired and wireless networks.

IP Address - In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IPCONFIG - A utility that provides for querying, defining and managing IP addresses within a network. A commonly used utility, under Windows NT and 2000, for configuring networks with static IP addresses.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A suite of protocols used to implement secure exchange of packets at the IP layer. IPSec supports two basic modes: Transport and Tunnel. Transport encrypts the payload of each packet, leaving the header untouched, while Tunnel mode encrypts both the header and the payload and is therefore more secure. IPSec must be supported on both transmitter and receiver and must share a public key. Tunnel mode is widely deployed in VPNs (Virtual Private Networks).

IRQ (**I**nterrupt **R**e**Q**uest) - A hardware interrupt on a PC. There are 16 IRQ lines used to signal the CPU that a peripheral event has started or terminated. Except for PCI devices, two devices cannot use the same line.

ISM band - The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

ISP - An ISP (Internet service provider) is a company that provides individuals and companies access to the Internet and other related services such as website building and virtual hosting.

LAN - A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the

resources of a single processor or server within a small geographic area (for example, within an office building).

Latency - The time delay between when the first bit of a packet is received and the last bit is forwarded.

MAC Address - The MAC (Media Access Control) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.
Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; unit of measurement for data transmission.

MD5 - A type of one-way authentication method that uses passwords. MD5 authentication is not as secure as the EAP-TLS or EAP/TTLS authentication methods. MD5 authentication does not support dynamic WEP key management.

MDI (**M**edium **D**ependent **I**nterface) - On a network hub or switch, a MDI port, also known as an uplink port, connects to another hub or switch using a straight-through cable. To connect a MDI port to a computer, use a crossover cable.

MDIX (**M**edium **D**ependent **I**nterface Crossed) - On a network hub or switch, a MDIX port connects to a computer using a straight-through cable. To connect a MDIX port to another hub or switch, use a crossover cable.

mIRC - mIRC runs under Windows and provides a graphical interface for logging onto IRC servers and listing, joining, and leaving channels.

Motherboard - A motherboard is the physical arrangement in a computer that contains the computer's basic circuitry and components.

Multicasting - Sending data to a group of nodes instead of a single destination.

NAT - NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

NetBEUI (**NetB**IOS **E**xtended **U**ser **I**nterface) - The transport layer for NetBIOS. NetBIOS and NetBEUI were originally part of a single protocol suite that was later separated. NetBIOS sessions can be transported over NetBEUI, TCP/IP, and IPX/SPX protocols.

NetBIOS - The native networking protocol in DOS and Windows networks. Although originally combined with its transport layer protocol (NetBEUI), NetBIOS today provides a programming interface for applications at the session layer (layer 5). NetBIOS can ride over NetBEUI, its native transport, which is not routable, or over TCP/IP and IPX/SPX, which are routable protocols.

NetBIOS computers are identified by a unique 15-character name, and Windows machines (NetBIOS machines) periodically broadcast their names over the network so that Network Neighborhood can catalog them. For TCP/IP networks, NetBIOS names are turned into IP addresses via manual configuration in an LMHOSTS file or a WINS server.

There are two NetBIOS modes. The Datagram mode is the fastest mode, but does not guarantee delivery. It uses a self-contained packet with send and receive name, usually limited to 512 bytes. If the recipient device is not listening for messages, the datagram is lost. The Session mode establishes a connection until broken. It guarantees delivery of messages up to 64KB long.

Network - A system that transmits any combination of voice, video, and/or data between users.

Network Mask - Also known as the “Subnet Mask.”

NIC (**N**etwork **I**nterface **C**ard) - A board installed in a computer system, usually a PC, to provide network communication capabilities to and from that computer system. Also called an adapter.

Node - A network junction or connection point, typically a computer or work station.

Notebook (PC) - A notebook computer is a battery-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, at temporary offices, and at meetings. A notebook computer, sometimes called a laptop computer, typically weighs less than five pounds and is three inches or less in thickness.

OFDM - Developed for wireless applications, Orthogonal Frequency Division Multiplexing (OFDM) technology offers superior performance-increased data rates and more reliable transmissions-than previous technologies, such as

DSSS. OFDM is a scheme in which numerous signals of different frequencies are combined to form a single signal for transmission on the medium.

OFDM works by breaking one high-speed data stream into a number of lower-speed data streams, which are then transmitted in parallel. Each lower speed stream is used to modulate a subcarrier. Essentially, this creates a multi-carrier transmission by dividing a wide frequency band or channel into a number of narrower frequency bands or sub-channels. OFDM is also used for other applications, including powerline networking.

Packet - A unit of data routed between an origin and a destination in a network.

Packet Filtering - Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.).

Partitioning - To divide a resource or application into smaller pieces.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

PC Card - A credit-card sized removable module that contains memory, I/O, or a hard disk.

PCI (**P**eripheral **C**omponent **I**nterconnect) - A peripheral bus commonly used in PCs, Macintoshes and workstations. It was designed primarily by Intel and first appeared on PCs in late 1993. PCI provides a high-speed data path between the CPU and peripheral devices (video, disk, network, etc.). There are typically three or four PCI slots on the motherboard. In a Pentium PC, there is generally a mix of PCI and ISA slots or PCI and EISA slots. Early on, the PCI bus was known as a “local bus.”

PCI provides “plug-and-play” capability, automatically configuring the PCI cards at startup. When PCI is used with the ISA bus, the only thing that is generally required is to indicate in the CMOS memory which IRQs are already in use by ISA cards. PCI takes care of the rest.

PCI allows IRQs to be shared, which helps to solve the problem of limited IRQs available on a PC. For example, if there were only one IRQ left over after ISA devices were given their required IRQs, all PCI devices could share it. In a PCI-only machine, there cannot be insufficient IRQs, as all can be shared.

PCMCIA - The PCMCIA (Personal Computer Memory Card International Association) is an industry group organized in 1989 to promote standards for a credit card-size memory or I/O device that would fit into a personal computer, usually a notebook or laptop computer.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Plug-and-Play - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

Port - A pathway into and out of the computer or a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems, and printers.

Port Mirroring - Port mirroring, also known as a roving analysis port, is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - PPPoE is a method for the encapsulation of PPP packets over Ethernet frames from the user to the ISP over the Internet. One reason PPPoE is preferred by ISPs is because it provides authentication (username and password) in addition to data transport. A PPPoE session can be initiated by either a client application residing on a PC, or by client firmware residing on a modem or router.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A protocol which allows the Point to Point Protocol (PPP) to be tunneled through an IP network. PPTP does not specify any changes to the PPP protocol but rather describes a “tunneling

service” for carrying PPP (a tunneling service is any network service enabled by tunneling protocols such as PPTP, L2F, L2TP, and IPSEC tunnel mode). One example of a tunneling service is secure access from a remote small office network to a headquarters corporate intranet via a Virtual Private Network (VPN) that traverses the Internet. However, tunneling services are not restricted to corporate environments and may also be used for personal (i.e., non-business) applications.

RIP (**R**outing **I**nformation **P**rotocol) - A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers.

RJ-11 (**R**egistered **J**ack-**11**) - A telephone connector that holds up to six wires. The RJ-11 is the common connector used to plug a telephone into a wall.

RJ-45 - A connector similar to a telephone connector that holds up to eight wires, used for connecting Ethernet devices.

Roaming - In an infrastructure mode wireless network, this refers to the ability to move out of one access point's range and into another and transparently reassociate and reauthenticate to the new access point. This reassociation and reauthentication should occur without user intervention and ideally without interruption to network connectivity. A typical scenario would be a location with multiple access points, where users can physically relocate from one area to another and easily maintain connectivity.

Router - Protocol-dependent device that connects subnetworks together. Routers are useful in breaking down a very large network into smaller subnetworks; they introduce longer delays and typically have much lower throughput rates than bridges.

RTS (**R**equest **T**o **S**end) - An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

Software - Instructions for the computer. A series of instructions that performs a particular task is called a “program.” The two major categories of software are “system software” and “application software.” System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user.

A common misconception is that software is data. It is not. Software tells the hardware how to process the data.

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

Spread Spectrum - Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

Static IP Address - A permanent IP address that is assigned to a node in a TCP/IP network.

Static Routing - Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

Storage - The semi-permanent or permanent holding place for digital data.

STP (**S**hielded **T**wisted **P**air) - Telephone wire that is wrapped in a metal sheath to eliminate external interference.

Subnet Mask - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

Swapping - Replacing one segment of a program in memory with another and restoring it back to the original when required.

Switch – 1. A data switch connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. TCP is known as a “connection oriented” protocol due to requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet resulting in transmission control.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

Telnet - A terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one place to another in a given time period.

Topology - A network’s topology is a logical characterization of how the devices on the network are connected and the distances between them. The most common network devices include hubs, switches, routers, and gateways. Most large networks contain several levels of interconnection, the most important of which include edge connections, backbone connections, and wide-area connections.

TX Rate – Transmission Rate.

UDP (**U**ser **D**atagram **P**rotocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. UDP is known as a "connection-less" protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP).

Upgrade - To replace existing software or firmware with a newer version.

Upload - To send a file transmitted over a network. In a communications session, upload means transmit, and download means receive.

URL (**U**niform **R**esource **L**ocator) - The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.

UTP - Unshielded twisted pair is the most common kind of copper telephone wiring. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable.

VPN (**V**irtual **P**rivate **N**etwork) - A technique that allows two or more LANs to be extended over public communication channels by creating private communication subchannels (tunnels). Effectively, these LANs can use a WAN as a single large "virtually private" LAN. This removes the need to use leased lines for WAN communications through secure use of a publicly available WAN (such as the Internet). Examples of VPN technology are: PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (Internet Protocol Security).

WAN (**W**ide **A**rea **N**etwork) - A communications network that covers a relatively large geographic area, consisting of two or more LANs. Broadband communication over the WAN is often through public networks such as the

telephone (DSL) or cable systems, or through leased lines or satellites. In its most basic definition, the Internet could be considered a WAN.

WEP (**W**ired **E**quivalent **P**rivacy) - A data privacy mechanism based on a 64-bit or 128-bi shared key algorithm, as described in the IEEE 802.11 standard.

WINIPCFG - Configuration utility based on the Win32 API for querying, defining, and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

Workgroup - Two or more individuals that share files and databases.

Appendix F: Specifications

Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, Draft 802.11g
Ports	
Internet:	One 10/100 RJ-45 Port for Cable/DSL Modem
LAN:	Four 10/100 RJ-45 Switched Ports One Power Port
Button	One Reset Button
Cabling Type	Category 5 Ethernet Network Cabling or better
Transmit Power	15 dBm
Modulation	
802.11b:	CCK, DQPSK, DBPSK
draft 802.11g:	OFDM
Network Protocols	TCP/IP , NetBEUI
LED Indicators	Power, DMZ, Diag
WLAN:	Act, Link
LAN:	Link/Act, Full/Col, 100
Internet:	Link/Act, Full/Col, 100

Environmental

Dimensions	7.32" x 6.89" x 1.89" (186 mm x 175 mm x 48 mm)
Unit Weight	17 oz. (0.482 kg)
Power	External, 5V DC, 2.5 A
Certifications	FCC Class B, CE Mark
Operating Temp.	0°C to 40°C (32°F to 104°F)
Storage Temp.	-20°C to 70°C (-4°F to 158°F)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing

Appendix G: Warranty Information

BE SURE TO HAVE YOUR PROOF OF PURCHASE AND A BARCODE FROM THE PRODUCT'S PACKAGING ON HAND WHEN CALLING. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE.

IN NO EVENT SHALL LINKSYS'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS DOES NOT OFFER REFUNDS FOR ANY PRODUCT.

LINKSYS OFFERS CROSS SHIPMENTS, A FASTER PROCESS FOR PROCESSING AND RECEIVING YOUR REPLACEMENT. LINKSYS PAYS FOR UPS GROUND ONLY. ALL CUSTOMERS LOCATED OUTSIDE OF THE UNITED STATES OF AMERICA AND CANADA SHALL BE HELD RESPONSIBLE FOR SHIPPING AND HANDLING CHARGES. PLEASE CALL LINKSYS FOR MORE DETAILS.

Appendix H: Contact Information

For help with the installation or operation of the Wireless-G Broadband Router, contact Linksys Technical Support at one of the phone numbers or Internet addresses below.

Sales Information	800-546-5797 (1-800-LINKSYS)
Technical Support	800-326-7114
RMA (Return Merchandise Authorization) Issues	www.linksys.com (or call 949-271-5461)
Fax	949-265-6655
E-mail	support@linksys.com
Web site	http://www.linksys.com
FTP site	ftp://ftp.linksys.com

www.linksys.com